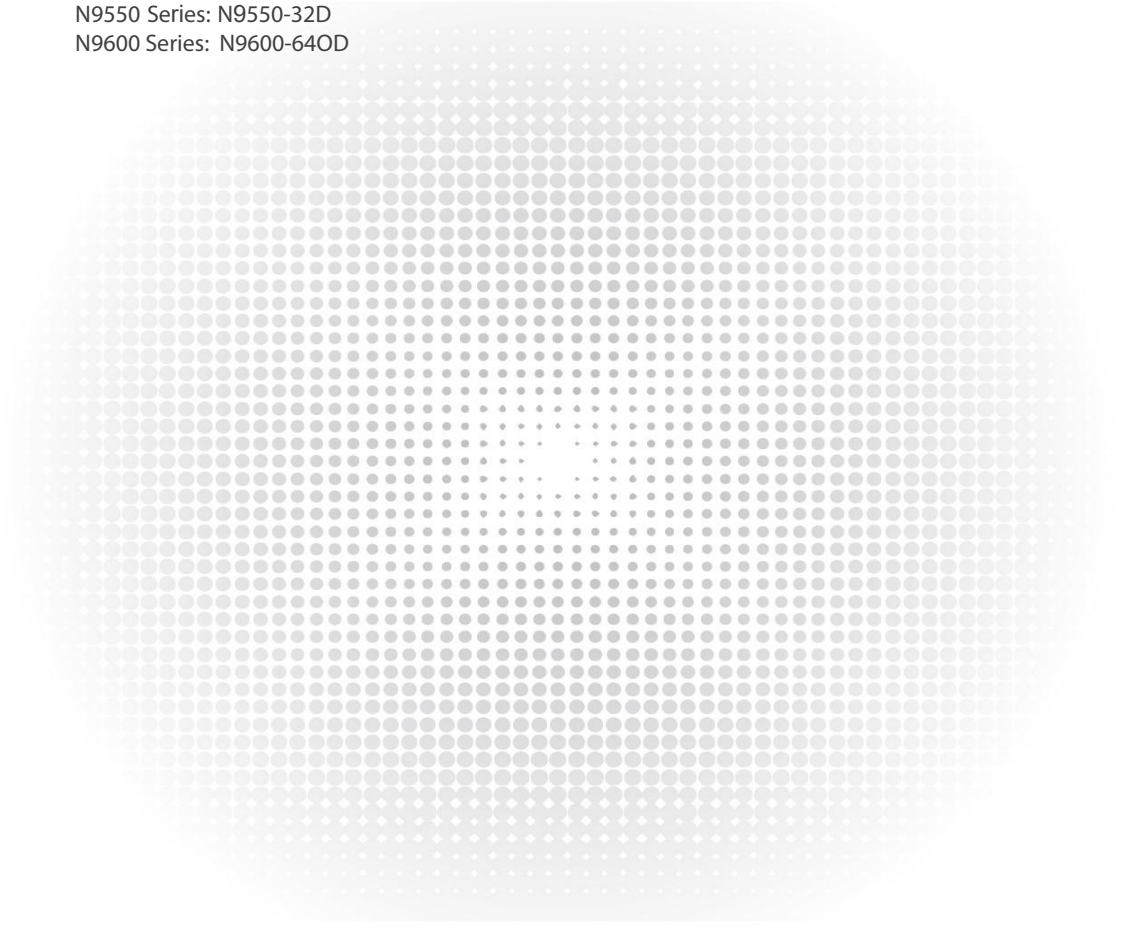
PicOS® Switches

Configuration Guide V4.5

Models:

S5810 Series: S5810-48TS-P; S5810-28TS; S5810-28FS; S5810-48TS; S5810-48FS
S5860 Series: S5860-20SQ; S5860-24XB-U; S5860-24MG-U; S5860-24XMG; S5860-48XMG-U; S5860-48XMG; S5860-48MG-U
S5870 Series: S5870-48T6S-U; S5870-48T6S; S5870-48T6BC-U; S5870-48T6BC; S5870-48MX6BC-U
N5850 Series: N5850-48S6Q; N5850-48X6C
N8550 Series: N8550-48B8C; N8550-32C; N8550-64C; N8550-24CD8D
N8560 Series: N8560-32C
N9550 Series: N9550-32D
N9600 Series: N9600-64OD



CONFIGURATION GUIDE

Release Notes for PICOS 4.5 . . . 15
Hardware Guides . . . 18
Hardware Compatibility . . . 19
FS Switch . . . 20
EdgeCore/Accton Switch . . . 24
Hardware Use Precautions . . . 26
AG5648/AS7312_54X/AS7312_54XS . . . 27
Dell N22xx Series Switches . . . 28
Limitation of Port Breakout . . . 29
Speed Setting on SFP28 Ports in a Quad-SerDes Core . . . 30
AS9716-32D Unsupported Features and Limitations . . . 31
N8560-32C Unsupported Features . . . 32
FS S5810 Series and S5860 Series Switch Unsupported Features . . . 33
S5860-48XMG-U/S5860-48XMG/S5860-48MG-U Limitation . . . 34
N9550-32D Unsupported Features and Limitations . . . 35
FS S3410 Series Switch Unsupported Features and Limitations . . . 36
N8560-64C Unsupported Features . . . 37
N8550-24CD8D Feature Support . . . 38
4.5.1E . . . 39
4.5.1.1 . . . 41
N9600-64OD Unsupported Features and Limitations . . . 42
Switch Machine Outline and System Characteristics . . . 43
Dell . . . 45
N2224X-ON/N2224PX-ON . . . 46
N3224F-ON . . . 48
Z9100-ON . . . 50
N2248X-ON/N2248PX-ON . . . 52
N3208PX-ON . . . 54
N3224P-ON//N3224T-ON . . . 56
N3224PX-ON . . . 59
N3248P-ON/N3248TE-ON . . . 61
N3248PXE-ON/N3248X-ON . . . 63
N3248TE-ON . . . 65
S4048 . . . 67
S4128F-ON/S4128T-ON . . . 69
S4148T-ON/S4148F-ON . . . 71
S5212F-ON . . . 73
S5224F-ON . . . 74
S5232F-ON . . . 76
S5248F-ON . . . 78
S5296F-ON . . . 80
Z9264F-ON . . . 82
EdgeCore/Accton . . . 84
AS7816-64X . . . 85
AS5835_54X . . . 86

AS9716-32D . . . 87
AS4610-30P . . . 88
AS4610-30T . . . 90
AS4610-54P . . . 91
AS4610-54T . . . 93
AS4625-54P/AS4625-54T . . . 94
AS4630-54NPE . . . 96
AS4630-54PE . . . 98
AS5712_54X/HP5712 . . . 100
AS5812_54T . . . 101
AS5812_54X . . . 102
AS5835_54T . . . 103
AS6812_32X . . . 104
AS7312_54X / AS7312_54XS . . . 105
AS7326-56X . . . 107
AS7712-32X . . . 108
AS7726-32X . . . 109
Delta/Agema . . . 110
AG9032v1 . . . 111
AG5648V1 . . . 112
AG7648 . . . 113
FS . . . 114
N8550-48B8C . . . 115
S5810-48TS-P . . . 116
S5810-28FS . . . 118
S5810-28TS . . . 120
S5810-48FS . . . 122
S5810-48TS . . . 123
S5860-20SQ . . . 124
S5860-24XB-U . . . 126
N8560-32C . . . 128
N8560-64C . . . 129
S5860-24MG-U . . . 130
S5860-48XMG-U . . . 132
S5860-48XMG . . . 134
S5860-24XMG . . . 136
S5860-48MG-U . . . 137
S5870-48T6S/S5870-48T6S-U . . . 139
S5870-48T6BC/S5870-48T6BC-U . . . 141
N5850-48X6C . . . 143
N8550-64C . . . 144
N9550-32D . . . 145
N5850-48S6C . . . 146
S5870-48MX6BC-U . . . 147
S3410-24TS . . . 149

S3410L-24TF . . . 150
S3410L-24TF-P . . . 151
S3410-24TS-P . . . 152
N8550-32C . . . 154
S3410C-8TMS-P . . . 155
S3410C-16TF . . . 156
N5850-48S6Q . . . 157
S3410C-16TMS-P . . . 158
S3410C-16TF-P . . . 159
S3410-48TS-P . . . 160
S3410-48TS . . . 162
S3410L-48TF . . . 163
N8550-24CD8D . . . 164
N9600-64OD . . . 166
Indicator Light on Switch Panel . . . 167
Dell Switches . . . 169
Z9100-ON Switch . . . 170
S4128F-ON/S4128T-ON Switch . . . 172
N3208PX-ON Switch . . . 175
N3224P-ON/N3224F-ON/N3224T-ON Switch . . . 177
N3224PX-ON Switch . . . 181
N3248P-ON/N3248TE-ON Switch . . . 184
N3248PXE-ON/N3248X-ON Switch . . . 187
N3248TE-ON Switch . . . 190
S4048 Switch . . . 193
S4148T-ON/S4148F-ON Switch . . . 195
S5212F-ON Switch . . . 198
S5224F-ON Switch . . . 200
S5248F Switch . . . 203
S5296F-ON Switch . . . 206
Z9264F-ON Switch . . . 208
S5232F-ON Switch . . . 210
N2224X-ON/N2224PX-ON Switch . . . 212
N2248X-ON/N2248PX-ON Switch . . . 215
EdgeCore/Accton Switches . . . 218
AS4610 Serial Switch . . . 219
AS4625-54P/AS4625-54T Switch . . . 220
AS4630-54NPE Switch . . . 221
AS7816-64X Switch . . . 223
AS5835-54X Switch . . . 225
AS4630-54PE Switch . . . 227
AS5712-54X Switch . . . 229
AS9716-32D Switch . . . 230
AS7312-54X/AS7312_54XS Switch . . . 232
AS5812-54T Switch . . . 234

AS5812-54X Switch . . . 236
AS5835-54T Switch . . . 238
AS6712-32X Switch . . . 241
AS6812_32X Switch . . . 243
AS7326-56X Switch . . . 245
AS7712-32X Switch . . . 247
AS7726-32X Switch . . . 249
Delta/Agema Switches . . . 251
AG9032v1 Switch . . . 252
AG5648V1 Switch . . . 254
AG7648 Switch . . . 256
FS Switches . . . 258
N5850-48S6C Switch . . . 259
N8550-32C Switch . . . 261
N5850-48S6Q Switch . . . 263
S5810-48TS-P Switch . . . 265
S5810-28FS Switch . . . 267
S5810-28TS Switch . . . 269
S5810-48FS Switch . . . 271
S5810-48TS Switch . . . 273
S5860-20SQ Switch . . . 275
S5860-24XB-U Switch . . . 277
N8560-32C Switch . . . 279
N8560-64C Switch . . . 280
S5860-24MG-U Switch . . . 282
S5860-48XMG-U Switch . . . 284
S5860-24XMG Switch . . . 286
S5860-48MG-U Switch . . . 288
S5860-48XMG Switch . . . 290
S5870-48T6S/S5870-48T6S-U Switch . . . 292
S5870-48T6BC/S5870-48T6BC-U Switch . . . 294
N5850-48X6C Switch . . . 296
N8550-64C Switch . . . 298
N9550-32D Switch . . . 300
S5870-48MX6BC-U Switch . . . 302
S3410-24TS Switch . . . 304
S3410L-24TF Switch . . . 305
S3410L-24TF-P Switch . . . 306
S3410-24TS-P Switch . . . 307
S3410C-8TMS-P Switch . . . 309
S3410C-16TF Switch . . . 311
S3410C-16TMS-P Switch . . . 312
S3410C-16TF-P Switch . . . 314
S3410-48TS-P Switch . . . 315
N8550-48B8C Switch . . . 317

S3410-48TS Switch . . . 319
S3410L-48TF Switch . . . 320
N8550-24CD8D Switch . . . 321
N9600-64OD Switch . . . 323
Port Index Description . . . 325
Dell Switch Port Name Description . . . 327
N2224X-ON/N2224PX-ON Switch Port Name Description . . . 328
N2248X-ON/N2248PX-ON Switch Port Name Description . . . 329
N3208PX-ON Switch Port Name Description . . . 331
N3224F-ON/N3224T-ON Switch Port Name Description . . . 332
N3224P-ON Switch Port Name Description . . . 333
N3224PX-ON Switch Port Name Description . . . 334
N3248P-ON/N3248TE-ON Switch Port Name Description . . . 335
N3248PXE-ON/N3248X-ON Switch Port Name Description . . . 337
S4048-ON Switch Port Name Description . . . 339
S4148T-ON Switch Port Name Description . . . 341
S5212F-ON Switch Port Name Description . . . 343
S5224F-ON Switch Port Name Description . . . 344
S5232F-ON Switch Port Name Description . . . 345
S5248F Switch Port Name Description . . . 346
S5296F-ON Switch Port Name Description . . . 348
Z9100-ON Switch Port Name Description . . . 351
Z9264F-ON Switch Port Name Description . . . 352
S4128F-ON Switch Port Name Description . . . 354
S4128T-ON Switch Port Name Description . . . 356
S4148F-ON Switch Port Name Description . . . 358
EdgeCore/Accton Switch Port Name Description . . . 361
AS5812_54T/AS5812_54X Switch Port Name Description . . . 362
AS4625-54P/AS4625-54T Switch Port Name Description . . . 364
AS4630-54NPE Switch Port Name Description . . . 366
AS4630-54PE Switch Port Name Description . . . 368
AS6812_32X Switch Port Name Description . . . 370
AS7312-54X/AS7312_54XS Switch Port Name Description . . . 371
AS7326-56X Switch Port Name Description . . . 373
AS7726-32X Switch Port Name Description . . . 376
AS7816-64X Switch Port Name Description . . . 378
AS9716-32D Switch Port Name Description . . . 380
AS4610_30T/AS4610_30P Switch Port Name Description . . . 382
AS4610_54T/AS4610_54P Switch Port Name Description . . . 384
AS5712_54X Switch Port Name Description . . . 387
AS5835_54X/AS5835_54T Switch Port Name Description . . . 389
AS7712_32X Switch Port Name Description . . . 391
Delta/Agema Switch Port Name Description . . . 393
AG5648V1 Switch Port Name Description . . . 394
AG7648 Switch Port Name Description . . . 396

AG9032v1 Switch Port Name Description 398
FS Switch Port Name Description 399
N5850-48S6Q Switch Port Name Description 400
N8550-32C Switch Port Name Description 402
N8550-48B8C Switch Port Name Description 404
S5810-48TS-P Switch Port Name Description 407
S5810-28FS Switch Port Name Description 409
S5810-28TS Switch Port Name Description 411
S5810-48FS Switch Port Name Description 413
S5810-48TS Switch Port Name Description 415
S5860-20SQ Switch Port Name Description 417
S5860-24XB-U Switch Port Name Description 419
N8560-32C Switch Port Name Description 421
N8560-64C Switch Port Name Description 423
S5860-24MG-U Switch Port Name Description 426
S5860-48XMG-U/S5860-48XMG Switch Port Name Description 428
S5860-24XMG Switch Port Name Description 430
S5860-48MG-U Switch Port Name Description 432
S5870-48T6S-U/S5870-48T6S Switch Port Name Description 434
S5870-48T6BC/S5870-48T6BC-U Switch Port Name Description 436
N5850-48X6C Switch Port Name Description 438
N8550-64C Switch Port Name Description 440
N9550-32D Switch Port Name Description 442
N5850-48S6C Switch Port Name Description 444
S5870-48MX6BC-U Switch Port Name Description 446
S3410-24TS Switch Port Name Description 448
S3410L-24TF Switch Port Name Description 450
S3410L-24TF-P Switch Port Name Description 452
S3410-24TS-P Switch Port Name Description 454
S3410C-16TMS-P Switch Port Name Description 455
S3410C-16TF-P Switch Port Name Description 456
S3410C-8TMS-P Switch Port Name Description 457
S3410C-16TF Switch Port Name Description 458
S3410-48TS-P Switch Port Name Description 459
S3410-48TS Switch Port Name Description 461
S3410L-48TF Switch Port Name Description 463
N8550-24CD8D Switch Port Name Description 465
N9600-64OD Switch Port Name Description 468
Switch Installation 481
Before Installation 482
Check the Installation Environment 483
Install and Remove FRU 484
Install and Remove RPSU 485
Installation 486
Install hangers, slide rail, grounding cable to the switch 487

Install the switch to the equipment cabinet . . . 488
The Switch installation flow chart . . . 489
Flow Scalability per Broadcom Chipset . . . 490
Switch Hardware Architecture . . . 492
PICOS System Configuration Guide . . . 493
Getting Started . . . 495
Boot Process and U-Boot Environment . . . 496
Configuring Password for Entering Linux Shell . . . 498
Initial Switch Access . . . 499
The Default Login . . . 502
Quick Configuration Guide . . . 505
Initial Setup . . . 506
Basic Configuration . . . 508
Network Configuration . . . 510
Configuring an Interface . . . 511
Configuring a loopback interface . . . 512
Configuring a Routed interface . . . 513
Configuring a VLAN Interface . . . 515
Configuring the Routing . . . 516
Configuring the Static Routing . . . 517
Configuring the Dynamic Routing . . . 518
Security Configuration . . . 520
Configuring an ACL . . . 521
Configuring the SSH Access . . . 523
Typical Configuration Example . . . 524
Installing or Upgrading PICOS . . . 529
ONIE Version and BIOS/U-Boot Information of Verified Platforms . . . 530
Installing PICOS on Bare Metal Switches . . . 537
Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command . . . 548
Upgrading PICOS from Version 3.0 or Later Using Upgrade2 . . . 557
Installing Debian Packages on PICOS . . . 569
Installing GCC on PicOS . . . 570
Installing Puppet on PicOS . . . 572
Installing Salt on PicOS . . . 574
PICOS Installation and Upgrade Guide for FS S5810 Series, S3410 Series, S5860 Series and N8560-32C Switches . . . 576
Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Console Port) . . . 577
Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Console Port) . . . 580
Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches . . . 587
Installing PICOS for FS S3410 Series Switches . . . 590
Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Eth0 or Inband Management Interface) . . . 592
Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Eth0 or Inband Management Interface) . . . 596
PICOS Debian Package Upgrade User Guide . . . 602
Zero Touch Provisioning (ZTP) . . . 604
Overview of ZTP . . . 605

ZTP Fundamentals 606

DHCP Configuration of ZTP . . . 608
Provision Script . . . 610
Enabling or Disabling ZTP . . . 618
Preparation before ZTP Deployment . . . 619
Example for Implementing ZTP Deployment through DHCP . . . 620
Appendix: ZTP API . . . 625
PICOS Licenses . . . 629
License Portal Guide . . . 630
Installing License under Linux prompt . . . 633
Installing and Removing License for PICOS go2cli Version . . . 641
PICOS Mode Selection . . . 643
Changing PicOS Mode by Modifying the Boot File . . . 644
PicOS Boot File . . . 646
Changing PicOS Mode from CLI . . . 648
PICOS Password Recovery . . . 653
Password Recovery for X86 Platform . . . 654
Password Recovery for AS4610 Series Switches . . . 658
Password Recovery Guide for FS S5810/S5860 Series Switches . . . 660
Password Recovery Guide for FS N8560-32C . . . 663
Setting Date and Time . . . 666
Boot Diagnosis Report . . . 668
Rebooting the System . . . 671
Auto-Run Script Upon System Boot Up . . . 672
Sample for Crossflow OVS Remarking Rules with Auto-run Script . . . 675
Graceful Bootup with Backup Configuration . . . 678
IP Rule of Management Network and Service Network . . . 679
Display System EEPROM Data Block . . . 683
Manual File Backup . . . 684
PICOS Monitor . . . 685
Enable Web-based Management Interface . . . 686
Linux command: ssh/scp/ping/traceroute/apt-get/telnet . . . 687
PICOS Open vSwitch Configuration Guide . . . 689
OpenFlow Support Matrix . . . 691
PicOS Support for OpenFlow 1.3 . . . 692
PicOS Support for OpenFlow 1.3.0 . . . 716
PicOS Support for OpenFlow 1.4 . . . 722
PicOS Support for OpenFlow 1.4.0 . . . 735
Introduction to Open vSwitch . . . 741
Introduction to OpenFlow . . . 743
OVS Web User Interface . . . 744
Login Interface . . . 745
Monitoring the Switch . . . 746
Adding a Bridge . . . 748
Add a Port . . . 749
Add GRE Port . . . 750

Add Group Table . . . 751
Add or Edit a Controller . . . 752
Edit Flow Tables . . . 753
Edit Lag Interface . . . 754
Configuring Open vSwitch . . . 755
Basic Configuration in OVS Mode . . . 757
Configuring sFlow v5 . . . 759
Configuring Port Mirroring . . . 760
OVSDB file . . . 761
OVS LLDP . . . 762
Enabling Radius in PicOS OVS Mode . . . 766
Inventory Database . . . 768
Broadcom Chip Limitation in OVS . . . 773
ARP Flow in Combinated Mode Table . . . 774
Overlap flow . . . 775
Priority of Arp flow . . . 776
Vlan Isolation . . . 778
Limitations on trident3 . . . 779
OVS CLI Enhancements . . . 780
Configuring Meter . . . 784
Configuration saving . . . 788
Configuring Buffer management . . . 790
Configuring snmp . . . 793
Configuring/Enabling SNMPv3 . . . 797
Configuring Precision Time Protocol . . . 799
Configuring Tunneling . . . 802
Configuring GRE . . . 803
Configuring L2GRE . . . 806
Configuring L2MPLS . . . 809
Configuring MPLS . . . 811
Configuring PBB . . . 815
Configuring QinQ . . . 816
Configuring VXLAN . . . 817
Match Vxlan VNI . . . 821
Multiple vxlan output port . . . 823
Decapsulation by pop actions . . . 826
Configuring Bridge and Ports . . . 827
Configuring bridge . . . 828
Configuring CDR . . . 832
Configuring CFM . . . 833
Configuring LFS . . . 837
Configuring Loopback . . . 839
Configuring ovs Remotely . . . 841
Configuring ports in bridge . . . 843
Configuring TPID in Port . . . 847

Configuring LAG and LACP . . . 849
Adding LAG and LACP . . . 850
GTP hash . . . 856
Lag hash . . . 857
Lag Resilient hash . . . 858
Symmetric Hashing in lag and ecmp . . . 860
Configuring QoS . . . 863
Configuring QoS scheduler . . . 864
CoS Mapping . . . 868
WRED . . . 870
Vlan Priority CoS Mapping . . . 873
Configuring Flow Table . . . 875
Combinated Mode . . . 876
Configuring ECMP . . . 877
Configuring egress flow table . . . 878
Configuring Flow Handling Mode . . . 879
Configuring Multi-Table . . . 881
Multitable Resources . . . 885
Configuring NAT flow . . . 889
Configuring option-match-vlan-type . . . 892
Configuring TTP . . . 893
TTP Multicast . . . 895
TTP Unicast . . . 899
Picos_ttp.json . . . 903
Configuring udf flow . . . 931
Match standard head in UDf mode . . . 935
Goto_table . . . 936
Optimizing TCAM Usage . . . 937
Configuring extend-group . . . 938
Configuring match-mode . . . 939
VN-tag . . . 942
Configuring Group . . . 944
Creating a Group Table . . . 945
Ecmp Select Group . . . 951
LAG Select Group . . . 953
Mirror Group . . . 954
Configuring Controller or Manager . . . 956
Connecting to a Controller . . . 957
Connecting to Manager . . . 961
Creating SSL Connection to a Controller . . . 963
Creating SSL Connection to a RYU Controller . . . 964
Configure OVS Connection Using SSL with Self-signed Certificates . . . 966
Configuring Counter . . . 970
Clear counter . . . 971
Drop counter . . . 972

Counter Interval . . . 976
Port Counter Interval . . . 977
Switching Open vSwitch version . . . 978
Configuring rate limit . . . 979
Configuring IPv4/IPv6 address for management port . . . 981
Configuring the Duplex Mode of Optical Port . . . 982
Configuring Port Speed on AS9716-32D and N9550-32D . . . 983
Examples and Topologies . . . 985
802.1Q VLAN . . . 986
ECMP . . . 987
GRE Tunnel . . . 988
MPLS Network . . . 989
Multiple Virtual Bridges . . . 991
SSL Connection to Controller . . . 992
PICOS OpenFlow Tutorials . . . 994
Basic Bridge Configuration . . . 995
Basic Bridge Introduction . . . 996
Power On Configuration . . . 997
Configure Switch . . . 999
Configure Bridge . . . 1000
Configure Port . . . 1002
Default Bridge Behavior . . . 1003
OVS Commands Reference . . . 1004
Basic Flow Configurations . . . 1005
Flow Introduction . . . 1006
Modify Default Flow . . . 1007
Uni-directional Flow . . . 1008
1-to-Many Multicasting . . . 1010
Many-to-One Aggregation . . . 1012
OVS Commands Used in this Tutorial . . . 1014
Packet Address File . . . 1015
Connection to a RYU Controller . . . 1016
RYU Introduction . . . 1017
Introduce RYU Open Flow Controller . . . 1018
Configure OVS for RYU OpenFlow Controller . . . 1019
Controller-OVS Interaction . . . 1020
RYU Simple Switch Application . . . 1022
Open Flow Message Type . . . 1024
RYU Guide OVS Commands Reference . . . 1025
Using TTP (router profile) with RYU Controller . . . 1026
Connection to OpenDaylight Controller . . . 1032
OpenDaylight Introduction . . . 1033
Introduction to the OpenDaylight OpenFlow Controller . . . 1034
Configure OVS for OpenDaylight Open Flow Controller . . . 1035
OpenDaylight Controller-OVS Interaction . . . 1036

OpenDaylight Simple Switch Application . . . 1038
Message Type of Open Flow . . . 1039
OVS Commands Reference 04 . . . 1040
Connection to a Floodlight Controller . . . 1041
Floodlight Controller Introduction . . . 1042
Floodlight Open Flow Controller . . . 1043
Test Topology . . . 1045
Configure OVS . . . 1046
Launch Floodlight . . . 1048
Floodlight REST Interface . . . 1050
Configuration Guide for Atrium Stack on ONOS Controller . . . 1051
ONOS Introduction . . . 1052
Installation Guide . . . 1054
ONOS Configuration Guide . . . 1056
Quagga Configuration Guide . . . 1059
PicOS Configuration Guide . . . 1062
How to Install ONOS . . . 1065
Feature Supported in PicOS OVS . . . 1069
Feature supported in different platform . . . 1070
Match fields supported . . . 1071
PICOS Open vSwitch Command Reference . . . 1073
ovs－appctl Commands . . . 1074
ovs-appctl Common Commands . . . 1075
ovs-appctl Help . . . 1076
ovs-appctl hwlog/set-level <module> <level> . . . 1077
ovs-appctl hwlog/set-type <mode> <type> . . . 1078
ovs-appctl ofproto/set_L34_enable . . . 1079
ovs-appctl Version . . . 1080
ovs-appctl vlog/list . . . 1081
ovs-appctl vlog/set . . . 1083
Pica8 Commands . . . 1084
ovs-appctl Target Commands . . . 1088
ovs-appctl -t ovs-vswitchd <command> . . . 1089
ovs－ofctl Commands . . . 1090
ovs-ofctl Common Commands . . . 1093
ovs-ofctl add-flow <bridge> <flow> . . . 1094
ovs-ofctl add-flows <bridge> <file> . . . 1099
ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions> . . . 1100
ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter> . . . 1102
ovs-ofctl bundle <bridge> <bundle> . . . 1103
ovs-ofctl del-flows <bridge> <flow> . . . 1105
ovs-ofctl del-group <bridge> [group_id=<id>] . . . 1106
ovs-ofctl del-meter <bridge> meter=<id> . . . 1107
ovs-ofctl del-meters <bridge> . . . 1108
ovs-ofctl dump-desc <bridge> . . . 1109

ovs-ofctl dump-flows <bridge> <flow> . . . 1110
ovs-ofctl dump-ports <bridge> <port> . . . 1111
ovs-ofctl dump-ports-desc <bridge> . . . 1112
ovs-ofctl dump-tables <bridge> . . . 1113
ovs-ofctl dump-tables-desc <bridge> . . . 1114
ovs-ofctl mod-flows <bridge> <flow> . . . 1115
ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions> . . . 1116
ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter> . . . 1117
ovs-ofctl mod－port <bridge> <iface> <action> . . . 1118
ovs-ofctl mod-table <bridge> <table> <mod> . . . 1119
ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]] . . . 1120
ovs-ofctl show <bridge> . . . 1121
ovs-ofctl snoop <bridge> . . . 1122
ovs-ofctl replace-flows <bridge> <file> . . . 1124
ovs-ofctl diff-flows <source1> <source2> . . . 1125
ovs-ofctl add-groups <bridge> <file> . . . 1126
ovs-ofctl queue-get-config <bridge> <port> . . . 1127
ovs-ofctl meter-stats <bridge> [meter] . . . 1128
ovs-ofctl meter-features <bridge> . . . 1129
ovs-ofctl dump-meters <bridge> . . . 1130
ovs－vsctl Commands . . . 1131
Bridge Commands . . . 1135
ovs-vsctl add-br . . . 1136
ovs-vsctl del-br . . . 1137
ovs-vsctl list-br . . . 1138
ovs-vsctl set bridge . . . 1139
Port Commands . . . 1140
ovs-vsctl add-port . . . 1142
ovs-vsctl list-ports . . . 1143
ovs-vsctl del-port . . . 1144
Controller commands . . . 1145
Database commands . . . 1146
Interface commands . . . 1150
Mirror Commands . . . 1151
NetFlow Commands . . . 1154
Open vSwitch commands . . . 1155
Match-mode Command . . . 1156
QoS_queue Commands . . . 1157
sFlow commands . . . 1158
Cos-map Command . . . 1159
Egress-mode Command . . . 1160
Set-flow-counter-mode Command . . . 1161
Combinated-mode Command . . . 1162
DSCP Commands . . . 1163
Troubleshooting Guide . . . 1164

L2/L3 Troubleshooting Guide . . . 1165
Monitoring and Debugging L2/L3 protocols . . . 1166
Routing and Forwarding Table . . . 1169
Using Pipe (|) Filter Functions . . . 1170
Using the show tech-support Command . . . 1172
PICOS OVS Troubleshooting . . . 1174
Debug while switch port cannot up . . . 1177
PICOS System Troubleshooting . . . 1179
Reset the Switch to Factory Default . . . 1181
Automating Ping to Multiple Hosts . . . 1182
Troubleshooting Switch Crashes . . . 1183
CPU/Memory Rate Limit . . . 1184
High CPU Utilization . . . 1185
Backup Partition for PicOS . . . 1188
SSH Server Preparation . . . 1189
Linux_configure.py script . . . 1190
Provision.py script . . . 1191
How to Disable Weak SSH Cipher/ MAC Algorithms in PICOS . . . 1192
Technical Support . . . 1196
General PICOS FAQ . . . 1197
Traceoptions Configuration Commands . . . 1198
Displaying the Debugging Message . . . 1199

Release Notes for PICOS 4.5

These notes summarize PICOS 4.5 new features, new hardware, known bugs, and bug fixes. Best practices recommend that you read all the content before upgrading to this release. For more detailed feature information, refer to the configuration guides.

PICOS 4.5.0E has been released as an **ESS (Early Sales Support)** stable version, aimed at supporting specific customer deployments and early adoption scenarios. This release provides early access to new features and enhancements tailored for targeted use cases. It serves as an intermediary step between internal testing and the General Availability (GA) release, enabling customers to explore and deploy features in controlled environments.

PICOS 4.5.1E version is an evaluation release specifically designed for the **N8550-24CD8D** platform. This release focuses on providing a foundational feature set but comes with certain limitations in functionality and usage. Please note that the current version supports only core features of the N8550-24CD8D platform, with some advanced capabilities not yet fully implemented or optimized.

PICOS 4.5.2E released as an ESS version for new platform N9600-64OD.

PICOS 4.5.0M2 is a GA release that brings enhanced stability and performance improvements. This version supports all platforms except S3410 series, S3270 series, N5860-48S6Q, N8550-24CD8D, and N9600-64OD switches, ensuring broader compatibility and reliability for network deployments.

Hardware

Ticket ID	Release	Description
-	4.5.2E	**Support FS Model N9600-64OD**
-	4.5.1E	**Support FS Model N8550-24CD8D**

New Features

Layer 2 and Layer 3

Ticket ID	Release	Description
-	4.5.0E	**IPv6 ND Inspection** IPv6 Neighbor Discovery (ND) Inspection is a security feature designed to enhance the protection of IPv6 networks by managing and validating Neighbor Discovery Protocol (NDP) messages, which are essential for the proper operation of IPv6 communication. Please have the details by reference document IPv6 Neighbor Discovery Inspection.
-	4.5.0E	**IPv6 ND Snooping** IPv6 Neighbor Discovery (ND) Snooping is a security feature that safeguards IPv6 networks to prevent various types of attacks. It functions similarly to ARP (Address Resolution Protocol) Snooping in IPv4 networks. Please have the details by reference document IPv6 Neighbor Discovery Snooping.
-	4.5.0E	**MPLS** MPLS (Multiprotocol Label Switching) operates between the link layer and the network layer in the TCP/IP protocol stack. It offers connectivity services to the IP layer while leveraging services from the link layer. Unlike traditional IP forwarding, MPLS uses label switching to direct traffic through the network. Please have the details by reference document MPLS Configuration.
-	4.5.0E	**PIM BSR (Bootstrap Router)** Dynamic RP allows multiple PIM devices within a PIM domain to be configured as C-RPs (Candidate RPs). Among these C-RPs, an RP is determined through an election process. The BSR aggregates information from all C-RPs in the network into an RP Set using Bootstrap messages and distributes it to all PIM devices. Each PIM device uses the RP Set to calculate and compare based on consistent rules, ultimately selecting an RP from the available C-RPs. Please have the details by reference document PIM Configuration Guide.
-	4.5.0E	**Ingress Buffer** Supports ingress buffer management, including guaranteed/shared/headroom management. Please have the details by reference document Configuring PFC Buffer.
-	4.5.0E	**PFC Watchdog Manual Control** The PFC Watchdog feature detects and resolves PFC (Priority Flow Control) deadlocks. Recovery methods include both automatic and manual recovery, allowing users to choose the appropriate approach for resolving deadlock scenarios. Please have the details by reference document Configuring PFC Watchdog.
-	4.5.0E	**PFC Deadlock Prevention** To avoid PFC deadlock issues, the DSCP value and corresponding Dot1p priority of the message can be modified so that the modified message can be forwarded using the new DSCP value in the new Dot1p priority queue, avoiding messages with the same DSCP value from remaining in PFC deadlock state. Please have the details by reference document Configuring PFC Deadlock Prevention.
-	4.5.0E	**Easy ECN** Explicit Congestion Notification (ECN) is a congestion notification mechanism operating at the IP and transport layers, serving as an extension to the TCP/IP protocol. With Easy ECN, users can enable WRED (Weighted Random Early Detection) policies, configure WRED thresholds, and set the maximum packet loss probability to manage network congestion more effectively. Please have the details by reference document Configuring Easy ECN.
-	4.5.0E	**DLB (Dynamic Load Balance)**

Ticket ID	Release	Description
		DLB breaks through the limitations of traditional static hash mechanisms by introducing timestamp and real-time load measurement factors (port bandwidth load, queue size) to optimize load balancing in both time and bandwidth space dimensions, providing a dynamic and intelligent hash mechanism. Please have the details by reference document Configuring Dynamic Load Balancing.
-	4.5.0E	**Standby IP Address** In cases where the management port cannot connect to the DHCP server and no static IP has been set through CLI during the switch's startup, it will default to using the secondary management IP address 192.168.1.1. This IP address serves as a backup, allowing management of the device even if DHCP services are unavailable. It is primarily used when the management port is directly connected to a PC, ensuring uninterrupted device management via this IP address. Please have the details by reference document Default Settings for Out-of-band Management Interface.
-	4.5.0E	**Perpetual PoE** Perpetual PoE (also known as hot-start uninterruptible power supply or permanent PoE) refers to the ability of Power Sourcing Equipment (PSE) to continue providing power during a system restart. This includes restarts initiated through CLI commands such as "request system reboot" or by rebooting under the Linux shell. Additionally, it supports uninterrupted power during system upgrades, including upgrades triggered via CLI or Linux-based upgrade methods. This feature ensures that PoE-powered devices remain operational even when the system is restarting or undergoing an upgrade. Please have the details by reference document Configuring Perpetual PoE.
-	4.5.0E	**PFC/ECN** GRPC monitoring PFC and ECN, in conjunction with gRPC, can provide PFC pause frame counts, PFC deadlock monitoring and ECN-marked packet counts for statistical queries. Please have the details by reference document PFC and ECN Statistical Reporting through gRPC.

Feature Enhancement

Ticket ID	Release	Description
-	4.5.0E	**DHCP Server Enhancement** In versions prior to 4.5.0E, clients were unable to obtain an address in a DHCP relay scenario. However, starting from version 4.5.0E, this issue has been resolved, and the system now fully supports DHCP address assignment in relay scenarios.
-	4.5.0E	**DHCP ZTP** After enabling the DHCP server with PicOS, address pools can be configured to allocate IP addresses to clients, along with additional network information such as gateway, DNS server addresses, log server addresses, TFTP server addresses, boot file names, and other options. These configurations are applied and synchronized with the clients as addresses are allocated. Please have the details by reference document Zero Touch Provisioning (ZTP).
	4.5.0E	**400G Port Splitting** The N9550-32D/AS9716-32D switches support the capability to split a 400G port into 2 * 200G and split to 4 * 100G ports, providing flexible bandwidth allocation for diverse network needs. Please have the details by reference document Configuring Port Breakout and Merge.
	4.5.0E	**PBR ECMP** PBR (Policy-Based Routing) action supports not only specifying a next-hop router or modifying DSCP values, but also enables the use of nexthop-group for ECMP (Equal-Cost Multi-Path) routing, allowing for more advanced and efficient traffic distribution across multiple paths. Please have the details by reference document Policy-Based Routing (PBR).

L2L3 WEB

Ticket ID	Release	Description
-	4.5.0E	**L2L3 WEB Access Control** Support is provided for using the command `set system services web disable` to modify the status of Layer 2 and Layer 3 WEB access, allowing administrators to enable or disable web access. The following switches support L2L3 WEB access, which is enabled by default: • S5810-48TS-P • S5810-28TS • S5810-28FS • S5810-48TS • S5810-48FS • S5860-20SQ • S5860-24XB-U • S5860-24MG-U • S5860-24XMG • S5860-48XMG-U • S5860-48XMG • S5860-48MG-U The following switches support L2L3 WEB access, but WEB access is disabled by default: • S5870-48T6S-U • S5870-48T6S • S5870-48MX6BC-U • S5870-48T6BC-U • S5870-48T6BC

Fixed Issues

Layer 2 and Layer 3

Ticket ID	Release	Description
18564	4.5.0M2	**[MLAG]** After configuring MLAG, the run show mlag link command always shows the link state as IDLE. This issue has been fixed
18446	4.5.0M2	**[MLAG/MLAG+EVPN]** After the MLAG peer restarts or reboots, the MLAG domain status stays at CONNECTING, while the peer shows ESTABLISHED. The issue is caus MLAG socket using the loopback address instead of the configured MLAG IP. This issue has been fixed.
15919	4.5.0M2	**[MLAG]** MLAG occasionally fails to reach FULL state, with error log: local0.err : [SIF]Socket 99 connect is in progress. This issue has been fixed.
17340	4.5.0M2	**[N8560-64C]** Port LED stays off even when the port is operational with an optical module installed.
17378	4.5.0E	**[DOT1X]** Setting the session timeout to 0 on the NAS and a non-zero session timeout on the NAC server causes a crash during 802.1X re-authentication. The bug is fixed in 4.5.0E.
17760	4.5.0M2	**[SNMP] LLDP Neighbor Information Retrieval Issue** When the number of LLDP neighbors exceeded five, SNMP failed to retrieve LLDP neighbor details. This issue has been fixed.
17386	4.5.0M2	**[LLDP] SNMP Notification Issue after Interface Reconfiguration** After enabling an interface by using command **set interface gigabit-ethernet** xx **disable true** and then disabling it by using command **delete interface gigabit-ethernet** xx **disable**, LLDP might not notify SNMP. This issue has been resolved.
17531	4.5.0M2	**[DHCP Server] Address Assignment Failure with Excessive Address Pools** In a direct connection scenario, configuring too many address pools caused the configuration file size to exceed 1024 characters, preventing the DHCP server from assigning IP addresses. This has been fixed.
17481	4.5.0M2	**[N9550-32D] Port LED Issue in Breakout Mode** When enabling breakout mode for 2×200G, the port LEDs did not illuminate. This issue has been addressed.
17544	4.5.0M2	**[CLI] No Output for Interface Command on AS9716-32D** On the AS9716-32D platform, executing the command **`run show interface gigabit-ethernet`** *`xe-1/1/xx`* and pressing Enter produced no output. This issue has been fixed.
17556	4.5.0M2	**[AS4610/N3024/N3048] System Crash when Handling Large Files** Copying or creating large files locally caused a *`core.bcmINTR`* error, leading to the *`pica_lcmgr`* process crashing. The kernel didn't report any errors, but PicOS restarted after some time. This issue has been fixed.
17330	4.5.0M2	**[S5850-48S6Q] High CPU Usage and Memory Leak Due to FPM Packet Handling** When receiving unknown packets, FPM discarded them but did not close the socket, leading to memory leaks and 100% CPU usage. This issue has been resolved.
17647	4.5.0M2	**[ACL - BCM] VRRP Virtual MAC Incorrectly Installed in ACL** In L2/L3 configurations, the VRRP virtual MAC (`00:00:5e`) was added to ACL even when VRRP was not configured, causing ping traffic destined for the VRRP MAC to be blocked. This issue has been fixed.
17366	4.5.0M2	**[SIF] VLAN Removal Issue Affecting Kernel Configuration** If a trunk port was configured with a native VLAN that was also a VLAN member, removing the native VLAN via CLI caused the kernel to incorrectly delete the VLAN, leading to VLAN anomalies. This issue has been fixed.
18806	4.5.0M2	**[N8550-32C] Cannot Correctly Read the SN (Serial Number) of the Power Module** When you execute the show system serial-number command on N8550-32C, the RPSU 1 Serial Number information cannot be displayed correctly. This issue has been fixed.
19136	4.5.0M2	**[MLAG N9550-32D] The MAC Learning Issue after the Counting Number Exceeds 8K** In the MLAG scenario of N9550-32D, due to the flaw in the SDK's MAC address counting mechanism, some MAC addresses are counted repeatedly. Even when the actual number of MAC entries has not reached the maximum capacity limit, the switch stops learning new MAC addresses. This issue has been fixed.

Known Limitations

Ticket ID	Release	Description
18171	4.5.2E	[N9600-64OD] Some sub-interfaces cannot come up in 8×50G mode when using the OSFP-SR8-800G module.
18400	4.5.2E	[N9600-64OD] The port light remains illuminated after the module is removed in port splitting mode.
18091	4.5.2E	[N9600-64OD] Undersized packets are not counted in the interface's 'Undersize Packets' statistics.
18504	4.5.2E	[N9600-64OD] The BMC light remains red after a successful system startup. PICOS does not control the BMC light. The light changes from flashing green to solid red.
18501	4.5.2E	**[N9600-64OD] Front Panel Ports 65 and 66 Not Supported** The two SFP front panel ports (65 and 66) are not adapted and are not supported in **4.5.2E**.
-	4.5.2E	[N9600-64OD] Packets smaller than 295 bytes will not reach full line rate due to hardware limitations.
-	4.5.2E	[N9600-64OD] This platform uses software-based MAC address learning, resulting in a slower learning rate compared to hardware-based platforms.
-	4.5.0M2	PICOS 4.5.0M does not support OSPF Multi-Instance.
-	4.5.0M2	PICOS 4.5.0M does not support telnet server.

Hardware Guides

- Hardware Compatibility
  - FS Switch
  - EdgeCore/Accton Switch
- Hardware Use Precautions
  - AG5648/AS7312_54X/AS7312_54XS
  - Dell N22xx Series Switches
  - Limitation of Port Breakout
  - Speed Setting on SFP28 Ports in a Quad-SerDes Core
  - AS9716-32D Unsupported Features and Limitations
  - N8560-32C Unsupported Features
  - FS S5810 Series and S5860 Series Switch Unsupported Features
  - S5860-48XMG-U/S5860-48XMG/S5860-48MG-U Limitation
  - N9550-32D Unsupported Features and Limitations
  - FS S3410 Series Switch Unsupported Features and Limitations
  - N8560-64C Unsupported Features
  - N8550-24CD8D Feature Support
  - N9600-64OD Unsupported Features and Limitations
- Switch Machine Outline and System Characteristics
  - Dell
  - EdgeCore/Accton
  - Delta/Agema
  - FS
- Indicator Light on Switch Panel
  - Dell Switches
  - EdgeCore/Accton Switches
  - Delta/Agema Switches
  - FS Switches
- Port Index Description
  - Dell Switch Port Name Description
  - EdgeCore/Accton Switch Port Name Description
  - Delta/Agema Switch Port Name Description
  - FS Switch Port Name Description
- Switch Installation
  - Install and Remove RPSU
  - Install and Remove FRU
  - Installation
  - Before Installation
  - Check the Installation Environment
- Flow Scalability per Broadcom Chipset
- Switch Hardware Architecture

Hardware Compatibility

We have listed all the supported hardware platforms and their ASIC types in a table by different hardware vendors. See details in the following pages.

- FS Switch
- EdgeCore/Accton Switch

FS Switch

List of FS Switches using Boot Installation
List of FS Switches using ONIE Installation

List of FS Switches using Boot Installation

Platform	ASIC Vendor	Chip	Switch ASIC	Port Configuration	CPU	License Type	Release	Installation
S5810-48TS-P	Broadcom	BCM56340	Helix4	48x1G copper 4x10G SFP+	ARM Cortex A9	1G	4.4.3.4	rboot
S5810-28TS	Broadcom	BCM56342	Helix4	28x1G copper 4x1G SFP 4x10G SFP+ The last 4x1G copper ports and 4x1G SFP ports are combo ports.	ARM Cortex A9	1G	4.4.3.4	rboot
S5810-28FS	Broadcom	BCM56342	Helix4	8x1G copper 28x1G SFP 4x10G SFP+ The 8x1G copper ports and first 8x1G SFP ports are combo ports.	ARM Cortex A9	1G	4.4.3.4	rboot
S5810-48TS	Broadcom	BCM56340	Helix4	48x1G copper 4x10G SFP+	ARM Cortex A9	1G	4.4.3.4	rboot
S5810-48FS	Broadcom	BCM56340	Helix4	48x1G SFP 4x10G SFP+	ARM Cortex A9	1G	4.4.3.4	rboot
S5860-20SQ	Broadcom	BCM56170	Hurricane3-MG	20x10G SFP+ 4x25G SFP28 2x40G QSFP+	ARM Cortex A9	10G	4.4.3.9	rboot
S5860-24XB-U	Broadcom	BCM56170	Hurricane3-MG	24x10G copper POE 4x10G SFP+ 4x25G SFP28	ARM Cortex A9	10G	4.4.3.9	rboot
N8560-32C	Broadcom	BCM56873	Trident 3	32x100G QSFP28	X86	100G	4.4.4	rboot
S5860-24MG-U	Broadcom	BCM56170	Hurricane3-MG	24x5G copper 4x25G SFP28	ARM Cortex A9	1G	4.4.4.1	rboot

S5860-24XMG	Broadcom	BCM56170	Hurricane3-MG	24x10G copper 4x10G SFP+ 4x25G SFP28	ARM Cortex A9	10G	4.4.4.1	rboot
S5860-48XMG-U	Broadcom	BCM56170	Hurricane3-MG	48x10G copper 4x25G SFP28 2x40G QSFP+	ARM Cortex A9	10G	4.4.4.1	rboot
S5860-48XMG	Broadcom	BCM56170	Hurricane3-MG	48x10G copper 4x25G SFP28 2x40G QSFP+	ARM Cortex A9	10G	4.4.4.1	rboot
S5860-48MG-U	Broadcom	BCM56170	Hurricane3-MG	48x5G copper 4x25G SFP28 2x40G QSFP+	ARM Cortex A9	1G	4.4.4.1	rboot
S3410-24TS-P	Broadcom	BCM56150	Hurricane2	24x1G copper POE 2x10G SFP+	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410-24TS	Broadcom	BCM56150	Hurricane2	24x1G copper 4x10G SFP+	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410L-24TF-P	Broadcom	BCM56152	Hurricane2	24x1G copper POE 4x1G SFP	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410L-24TF	Broadcom	BCM56152	Hurricane2	24x1G copper 4x1G SFP	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410C-8TMS-P	Broadcom	BCM56150	Hurricane2	2x5G/2.5G/1G copper POE 8x1G/100M/10M copper 2x10G/1G SFP+ The first 6x1G/100M/10M copper ports support POE.	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410C-16TF	Broadcom	BCM56150	Hurricane2	16x1G/100M/10M copper 2x1G SFP	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410C-16TF-P	Broadcom	BCM56150	Hurricane2	16x1G/100M/10M copper (First 8 copper port support POE) 2x1G SFP	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410C-16TMS-P	Broadcom	BCM56150	Hurricane2	2x5G/2.5G/1G copper POE 16x1G/100M/10M copper (First 6x1G/100M/10M copper port support POE) 2x10G/1G SFP+	ARM Cortex A9	1G	4.4.5.1-beta	uboot
S3410-48TS-P	Broadcom	BCM56150	Hurricane2	24x1G/100M/10M copper POE 2x10G/1G SFP+	ARM Cortex A9	1G	4.4.5.10	uboot

S3410-48TS	Broadcom	BCM56150	Hurricane2	48x1G/100M/10M copper 4x10G SFP+	ARM Cortex A9	1G	4.4.5.10	uboot
S3410L-48TF	Broadcom	BCM56152	Hurricane2	48x1G/100M/10M copper 4x1G SFP	ARM Cortex A9	1G	4.4.5.10	uboot

List of FS Switches using ONIE Installation

Platform	ASIC Vendor	Chip	Switch ASIC	Port Configuration	CPU	License Type	Release	Installation
N5850-48S6Q	Broadcom	BCM56864	Trident2+	48 x 10G 6 x 40G	Intel x86	10G	4.4.3	ONIE
N8550-48B8C	Broadcom	BCM56870	Trident3-X7	48 x 25G 8 x 100G	Intel x86	25G	4.4.3	ONIE
N8550-32C	Broadcom	BCM56870	Trident3-X7	32 x 100G	Intel x86	100G	4.4.3	ONIE
S5870-48T6S-U	Broadcom	BCM56277	Trident3-X2	48 x 1G PoE + 6 x 10G	Intel x86	1G	4.4.4.2	ONIE
S5870-48T6S	Broadcom	BCM56277	Trident3-X2	48 x 1G-T + 6 x 10G	Intel x86	1G	4.4.4.2	ONIE
S5870-48T6BC-U	Broadcom	BCM56371	Trident3-X3	48 x 1G PoE + 4 x 25G +2 x 100G	Intel x86	1G	4.4.4.2	ONIE
S5870-48T6BC	Broadcom	BCM56371	Trident3-X3	48 x 1G + 4 x 25G +2 x 100G	Intel x86	1G	4.4.4.2	ONIE
N5850-48X6C	Broadcom	BCM56771	Trident3-X5	48 x 10G-T + 6 x 100G	Intel x86	10G	4.4.4.4	ONIE
N8550-64C	Broadcom	BCM56970	Tomahawk 2	64 x 100G	Intel x86	100G	4.4.5	ONIE
N9550-32D	Broadcom	BCM56980	Tomahawk III	32 x 400G	Intel x86	400G	4.4.5	ONIE
S5870-48MX6BC-U	Broadcom	BCM56371	Trident3-X3	36 x 1/2.5G PoE + 12 x 1/2.5/5/10G PoE + 4 x 25G +2 x 100G	Intel x86	1G	4.4.5	ONIE
N5850-48S6C	Broadcom	BCM56771	Trident3-X5	48 x 10G + 6 x 100G	Intel x86	10G	4.4.5	ONIE
N8560-64C	Broadcom	BCM56970	Tomahawk 2	64 x 100G	Intel x86	100G	4.4.5	ONIE

N8550-24CD8D	Broadcom	BCM56780	Trident4-X9	24 x 200G 8 x 400G	Intel x86	200G	4.5.1E	ONIE
N9600-64OD	Broadcom	BCM78900	Tomahawk 5	64 x 800G	Intel x86	800G	4.5.2E	ONIE

EdgeCore/Accton Switch

Product	Model	Configuration	Switch ASIC	CPU
100G Switch Portfolio	AS7726-32X (DCS204)	32 x 100G	Trident 3×7	Intel x86
100G Switch Portfolio	AS7712-32X (DCS501)	32 x 100G	Tomahawk	Intel x86
100G Switch Portfolio	AS7816-64X (DCS500)	64 x 100G	Tomahawk 2	Intel x86
40G Switch Portfolio	AS6701-32X	32 x 40G	Trident II	Power PC
40G Switch Portfolio	AS6712-32X	32 x 40G	Trident II	Intel x86
40G Switch Portfolio	AS6812-32X	32 x 40G	Trident II+	Intel x86
25G Switch Portfolio	AS7326-56X (DCS203)	48 x 25G 8 x 100G	Trident 3×7	Intel x86
25G Switch Portfolio	AS7312-54XS	48 x 25G 6 x 100G	Tomahawk +	Intel x86
10G Switch Portfolio	AS5835-54T (DCS209)	48 x 10G-T 6 x 100G	Trident III	Intel x86
10G Switch Portfolio	AS5835-54X (DCS208)	48 x 10G 6 x 100G	Trident III	Intel x86
10G Switch Portfolio	AS5812-54T	48 x 10G-T 6 x 40G	Trident II+	Intel x86
10G Switch Portfolio	AS5812-54X	48 x 10G 6 x 40G	Trident II+	Intel x86
10G Switch Portfolio	AS5712-54X	48 x 10G 6 x 40G	Trident II	Intel x86
Multi-Gig Switch Portfolio	AS4630-54NPE (EPS203)	36 x 1/2.5G PoE 12 x 1/2.5/5/10G PoE	Trident III	Intel x86
1G Switch Portfolio	AS4630-54PE (EPS202)	48 x 1G PoE 4 x 25G	Trident III	Intel x86
1G Switch Portfolio	AS4630-54TE (EPS201)	48 x 1G 4 x 25G	Trident III	Intel x86
1G Switch Portfolio	AS4610-54P	48 x 1G PoE 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-30P	24 x 1G PoE 4 x 10G	Helix4	ARM Cortex A9

1G Switch Portfolio	AS4610-54T	48 x 1G-T 4 x 10G	Helix4	ARM Cortex A9
1G Switch Portfolio	AS4610-30T	24 x 1G-T 4 x 10G	Helix4	ARM Cortex A9
400G Switch Portfolio	AS9716-32D	32 x 400G	Tomahawk III	Intel x86
1G Switch Portfolio	AS4625-54P	48 x 1G PoE 6 x 10G	Trident3-X2	Intel x86
1G Switch Portfolio	AS4625-54T	48 x 1G-T 6 x 10G	Trident3-X2	Intel x86

Hardware Use Precautions

This document describes the precautions related to hardware you must take when using.

- AG5648/AS7312_54X/AS7312_54XS
- Dell N22xx Series Switches
- Limitation of Port Breakout
- Speed Setting on SFP28 Ports in a Quad-SerDes Core
- AS9716-32D Unsupported Features and Limitations
- N8560-32C Unsupported Features
- FS S5810 Series and S5860 Series Switch Unsupported Features
- S5860-48XMG-U/S5860-48XMG/S5860-48MG-U Limitation
- N9550-32D Unsupported Features and Limitations
- FS S3410 Series Switch Unsupported Features and Limitations
- N8560-64C Unsupported Features
- N8550-24CD8D Feature Support
- N9600-64OD Unsupported Features and Limitations

AG5648/AS7312_54X/AS7312_54XS

Follow the below precautions before using AG5648/AS7312_54X/AS7312_54XS switch:

1. The first 48 ports are grouped, each four ports are grouped as shown in the following table.

Groups of ports	port1- port4	port5- port8	port9- port12	port13- port16	port17- port20	port21- port24
	port25- port28	port29- port32	port33- port36	port37- port40	port41- port44	port45- port48

2. When configuring the port rate, the supported rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports in the same group can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for the group of ports.

	te-1/1/21	**te-1/1/22**	**te-1/1/23**	**te-1/1/24**	**Allowed or not allowed**
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Dell N22xx Series Switches

- IPv6 is not supported on Dell N22xx series switches.
- GRE is not supported on Dell N22xx series switches.

Limitation of Port Breakout

Due to ASIC limitation, there are some 100GE interfaces on certain platforms do not support port splitting. The following table gives a summary.

> **NOTE:**
> For AS7726-32X, AS7326-56X, N8550-48B8C and N8550-32C, by default, there are no such limitation described in the below table. The limitation of port breakout only happens when the 10G-Base-KR ports are enabled as either front panel ports or management ports. For details about 10G-Base-KR ports, see 10G-Base-KR Interface Configuration.

Platform	Limitation Description
AS6812_32X	Ports xe-1/1/13, xe-1/1/14, xe-1/1/15, xe-1/1/16, xe-1/1/29, xe-1/1/30, xe-1/1/31 and xe-1/1/32 are not allowed to be split into four Gigabit Ethernet ports.
AS5835_54X/AS5835_54T/ N5850-48X6C	Only ports xe-1/1/1 and xe-1/1/4 can be split into four Gigabit Ethernet ports, other ports are not allowed to be split.
AS7726-32X	Port xe-1/1/32 is not allowed to be split into four Gigabit Ethernet ports.
N8550-32C	Port xe-1/1/32 is not allowed to be split into four Gigabit Ethernet ports.
AS7326-56X	Port xe-1/1/8 is not allowed to be split into four Gigabit Ethernet ports.
N8550-48B8C	Port xe-1/1/8 is not allowed to be split into four Gigabit Ethernet ports.
S5232F-ON	Port xe-1/1/32 is not allowed to be split into four Gigabit Ethernet ports.
AS7816-64X	Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet ports.
N8550-64C	Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet ports.
Z9264F-ON	Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet ports.

Speed Setting on SFP28 Ports in a Quad-SerDes Core

For the 4 ports in a single Quad-SerDes Core, the default speed are set to 25G. And auto detection of the speed is disabled. The four port can link up only if set the speed of all the four ports to either 25G or 10G/1G. This new additions would cover AS7312, N3248PXE, S5248, AS7326 and N3248EPX.

AS9716-32D Unsupported Features and Limitations

Unsupported Features

The following features are not supported on AS9716-32D:

- MAC-based VLAN
- QinQ
- PVLAN
- Mirror output port cannot be a LAG port.
- Regular Hashing for LAGs
- Resilient Hashing for LAGs
- Storm Control
- Egress meter
- Routed interface with VRF
- VxLAN/L2-GRE/L2-MPLS/PBB (Provider Backbone Bridge)
- Interface STM share mode
- OVS ICAP doesn’t support modifying src/dst MAC
- OVS NAT flow
- OVS UDF v2
- OVS L2/L3 buffer mode

Limitations

PICOS has the following limitations on AS9716-32D:

- LAG hash only supports advance mode and symmetric mode
- Only support QoS egress queue 0-3
- Firewall filter copp cannot configure policer on AS9716-32D.

For example,

```
admin@PICOS# set firewall filter copp sequence 100 then policer p1
admin@PICOS# commit
Filter copp can't configure policer in current platform
Commit failed.
```

N8560-32C Unsupported Features

The following OVS and L2/L3 features are not supported on FS N8560-32C switch:

- UDFv1
- Egress meter
- match-vlan-type
- VN-Tag
- Rate limit
- Push VLAN for QinQ packets

FS S5810 Series and S5860 Series Switch Unsupported Features

- The following OVS features are not supported on FS S5810 Series and S5860 Series switch:
  - Vxlan
  - MPLS/L2MPLS
  - PBB
  - Flexible mode
  - NAT
  - GTP Hash
  - Resilient hash
  - Match-vlan-type(vlan format)
  - udfv2
  - Match vxlan vni
  - Xlate table of TTP
- The following L2/L3 features are not supported on FS S5810 Series and S5860 Series switch:
  - GRE
  - VxLAN
  - IPFIX
- DHCP snooping has the following limiation:

DHCP snooping binding file which is set by command **set protocols dhcp snooping binding file** <*file-path*> does not work now.

NOTE:

GRE function is not supported on S5860 Series switches but supported on S5810 Series switches.

S5860-48XMG-U/S5860-48XMG/S5860-48MG-U Limitation

The S5860-48XMG-U/S5860-48XMG/S5860-48MG-U switches are dual-chip switches which flood received broadcast, multicast, or unknown unicast traffic between chips. When there is a large amount of broadcast, multicast, or unknown unicast traffic, it may trigger an intra-device broadcast storm, resulting in inter-chip network congestion and packet loss.

N9550-32D Unsupported Features and Limitations

Unsupported Features

The following features are not supported on N9550-32D:

- MAC-based VLAN
- QinQ
- PVLAN
- Mirror output port cannot be a LAG port.
- Regular Hashing for LAGs
- Resilient Hashing for LAGs
- Storm Control
- Egress meter
- Routed interface with VRF
- VxLAN/L2-GRE/L2-MPLS/PBB (Provider Backbone Bridge)
- Interface STM share mode
- OVS ICAP doesn’t support modifying src/dst MAC
- OVS NAT flow
- OVS UDF v2
- OVS L2/L3 buffer mode

Limitations

PICOS has the following limitations on N9550-32D:

- LAG hash only supports advance mode and symmetric mode.
- Only support QoS egress queue 0-3.
- Firewall filter copp cannot configure policer on N9550-32D.

For example,

```
admin@PICOS# set firewall filter copp sequence 100 then policer p1
admin@PICOS# commit
Filter copp can't configure policer in current platform
Commit failed.
```

FS S3410 Series Switch Unsupported Features and Limitations

- The following L2/L3 features are not supported on S3410 Series switch:
  - not support IS-IS
  - not support OSPFv2/OSPFv3 GR
  - not support IPv6 Source Guard
  - not support IPv6 DHCP Guard
  - not support IPv6 DHCP Snooping
  - not support PFC Watchdog
  - not support ECMP Hash Mode (Randomized Load Balance, Round-Robin Load Balance and Dynamic Load Balance Normal Mode)
  - not support L3 GRE
  - not support VXLAN
  - not support IGMP
  - not support PIM
  - not support buffer dynamic shared for egress multicast queue
  - not support symmetric hash
  - not support resilient hash
  - not support advance hash
  - not support PFC (Priority Flow Control)
  - not support ECMP
  - not support NETCONF
  - not support VRF
  - not support CoPP max bandwidth and min bandwidth configuration
- S3410 Series switches do not support OVS (Open vSwitch).
- S3410 Series switches do not support CrossFlow.
- S3410 Series switches do not support installing through USB.
- When upgrading, the S3410 Series switches only support the **upgrade2** method and do not support the **upgrade** method. For detailed instructions of **upgrade2**, please refer to:

PICOS Installation and Upgrade Guide for FS S5810 Series, S3410 Series, S5860 Series and N8560-32C Switches

- The commands **sudo systemctl stop picos** and **sudo systemctl restart picos** are not supported on S3410 Series switches.
- S3410 Series switches do not have an Eth0 management port; instead, an in-band management port is used. By default, the in-band management function of all the service port is enabled on VLAN 1 with a system built-in interface name *inband-mgmt*. For more details, see document Default Settings for In-Band Management Interface on S3410 Series Switches .
- The loopback port cannot establish BGP neighbors, resulting in routing function cannot work on S3410 Series switches.
- Only up to two concurrent SSH connections can be active at the same time. The idle timeout for SSH sessions is fixed to 3600s.

S3410 Series Switch File Storage Guidelines

- **Small Files**
  - It is recommended to store small files in the `/home/admin/` directory or the default `/cftmp/` directory.
- **Large Files (e.g., Image Files)**
  - Due to limited space in `/home/admin/` and `/cftmp/`, large files should be stored in the `/mnt/open/` directory.
- **Directory Cleanup**
  - To maintain system cleanliness and ensure efficient operation, please delete unnecessary files promptly.

N8560-64C Unsupported Features

The following OVS and L2/L3 features are not supported on FS N8560-64C switch:

- VXLAN routing
- OVS MPLSv1
- OVS VLANv1
- Resilient hashing for LAGs

N8550-24CD8D Feature Support

- 4.5.1E
- 4.5.1.1

4.5.1E

The 4.5.1E version provides a foundational feature set tailored to N8550-24CD8D platform but includes certain limitations in functionality and usage.

It is important to note that the 4.5.1E release focuses on delivering core features for the N8550-24CD8D platform, with some advanced capabilities not yet fully implemented or optimized. Further improvements and feature expansions for the platform will be based on user feedback and testing results, and are planned for upcoming software releases.

The detailed feature support for the N8550-24CD8D in version 4.5.1E is listed below.

Supported Features List

The following features are supported on N8550-24CD8D:

- FDB (Forwarding Database)
- FlexLink
- VRRPv2 (Virtual Router Redundancy Protocol)/VRRPv3/Active VRRP
- ARP (Address Resolution Protocol)/IPv6 Neighbor Discovery
- Undersize/Oversize
- LACP (Link Aggregation Control Protocol)
- IEEE 802.1Q
- SNMPv2 (Simple Network Management Protocol) /SNMPv3
- MSTP (Multiple Spanning Tree Protocol)/ PVST (Per-VLAN Spanning Tree) / RSTP (Rapid Spanning Tree Protocol)
- Mirror
- ERSPAN (Encapsulated Remote SPAN）
- VLAN Range
- NETCONF
- LAG hash
- Resilient LAG hash
- Static Route IPv4/IPv6
- IPv6 Function
- AAA（TACACS / RADIUS）
- SFlow
- VRF (Virtual Routing Forwarding)
- OSPF (Open Shortest Path First) /OSPF VRF
- RIP (Routing Information Protocol)
- DHCP (Dynamic Host Configuration Protocol) Snooping
- CoPP (Control Plane Policing)
- Routed Interface

Unsupported Features List

The following features are not supported on N8550-24CD8D:

- LAG symmetric hash
- DHCP Relay
- ARP Inspection

- IGMPv2 (Internet Group Management Protocol)/IGMPv3
- IGMP Snooping
- Voice VLAN
- LLDP (Link Layer Discovery Protocol)
- Buffer Management
- ECMP (Equal-Cost Multipath Routing) hash
- ECMP symmetric hash
- BPDU (Bridge Protocol Data Unit) Tunnel
- GRE (Generic Routing Encapsulation)
- Sub-interface
- Port-Security
- QinQ (802.1Q-in-802.1Q)
- RA Guard
- STM (Synchronous Transfer Mode)
- PIM (Protocol Independent Multicast)
- Storm/Stormratio/Stormcktbps
- Flow Control
- Counter
- PTP (Precision Time Protocol）
- VXLAN
- MAC-based VLAN
- MLAG

4.5.1.1

Version 4.5.1.1 builds upon the foundational 4.5.1E release, introducing expanded functionality and optimizations for the N8550-24CD8D platform. This release focuses on enhancing performance and usability while providing initial support for some advanced features. This release provides critical functionality validation support for the official GA of the N8550-24CD8D platform.

Expanded support for advanced networking features as listed below:

- MLAG (support MLAG + VRRP)
- PFC
- ECMP (Equal-Cost Multipath Routing) hash
- ECMP symmetric hash
- LAG symmetric hash
- LLDP (Link Layer Discovery Protocol)
- Buffer Management

N9600-64OD Unsupported Features and Limitations

Unsupported Features

The following features are not supported on N9600-64OD:

- MAC-based VLAN
- QinQ
- Voice VLAN
- IPv6 ND Inspection
- EFM OAM
- PTP-TC
- sFlow
- IGMP snooping
- Private VLAN
- VXLAN
- RA Guard
- EVPN
- MPLS
- IPv6SG (IPv6 Source Guard)

Switch Machine Outline and System Characteristics

- Dell
  - N2224X-ON/N2224PX-ON
  - N3224F-ON
  - Z9100-ON
  - N2248X-ON/N2248PX-ON
  - N3208PX-ON
  - N3224P-ON//N3224T-ON
  - N3224PX-ON
  - N3248P-ON/N3248TE-ON
  - N3248PXE-ON/N3248X-ON
  - N3248TE-ON
  - S4048
  - S4128F-ON/S4128T-ON
  - S4148T-ON/S4148F-ON
  - S5212F-ON
  - S5224F-ON
  - S5232F-ON
  - S5248F-ON
  - S5296F-ON
  - Z9264F-ON
- EdgeCore/Accton
  - AS7816-64X
  - AS5835_54X
  - AS9716-32D
  - AS4610-30P
  - AS4610-30T
  - AS4610-54P
  - AS4610-54T
  - AS4625-54P/AS4625-54T
  - AS4630-54NPE
  - AS4630-54PE
  - AS5712_54X/HP5712
  - AS5812_54T
  - AS5812_54X
  - AS5835_54T
  - AS6812_32X
  - AS7312_54X / AS7312_54XS
  - AS7326-56X
  - AS7712-32X
  - AS7726-32X
- Delta/Agema
  - AG9032v1
  - AG5648V1
  - AG7648
- FS
  - N8550-48B8C
  - S5810-48TS-P
  - S5810-28FS
  - S5810-28TS
  - S5810-48FS
  - S5810-48TS
  - S5860-20SQ
  - S5860-24XB-U
  - N8560-32C
  - N8560-64C
  - S5860-24MG-U
  - S5860-48XMG-U
  - S5860-48XMG
  - S5860-24XMG
  - S5860-48MG-U
  - S5870-48T6S/S5870-48T6S-U
  - S5870-48T6BC/S5870-48T6BC-U
  - N5850-48X6C
  - N8550-64C
  - N9550-32D

- N5850-48S6C
- S5870-48MX6BC-U
- S3410-24TS
- S3410L-24TF
- S3410L-24TF-P
- S3410-24TS-P
- N8550-32C
- S3410C-8TMS-P
- S3410C-16TF
- N5850-48S6Q
- S3410C-16TMS-P
- S3410C-16TF-P
- S3410-48TS-P
- S3410-48TS
- S3410L-48TF
- N8550-24CD8D
- N9600-64OD

Dell

- N2224X-ON/N2224PX-ON
- N3224F-ON
- Z9100-ON
- N2248X-ON/N2248PX-ON
- N3208PX-ON
- N3224P-ON//N3224T-ON
- N3224PX-ON
- N3248P-ON/N3248TE-ON
- N3248PXE-ON/N3248X-ON
- N3248TE-ON
- S4048
- S4128F-ON/S4128T-ON
- S4148T-ON/S4148F-ON
- S5212F-ON
- S5224F-ON
- S5232F-ON
- S5248F-ON
- S5296F-ON
- Z9264F-ON

N2224X-ON/N2224PX-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 1GbE/2.5GbE RJ45 port	(8) 25GbE SFP28	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) 40GbE QSFP	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
1GbE/2.5GbE RJ45 port	24
25GbE SFP28	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
RJ45 port LED	1 x 24
25GbE SFP28 LED	2 x 4
40GbE QSFP	2
40GbE QSFP LED	2 x 2

Micro-USB	1
USB port	1
Reset button	1
PSU	2
FAN	2

***UPoE**

The last 12 RJ45 ports on the front panel of N2224PX-ON support UPoE, the maximum output power can be set to up to 60 watts. The first 12 RJ45 ports support PoE but not UPOE, the maximum output power can be set to up to 30 watts.

25GbE SFP28 Port

Ports Te-1/1/25, Te-1/1/26, Te-1/1/27 and Te-1/1/28 are a group of ports, you should manually configure the port speed for these four ports by using the set interface gigabit-ethernet speed command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/25	**te-1/1/26**	**te-1/1/27**	**te-1/1/28**	**Allowed or not allowed**
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	X
case #6	25G	10G	25G	10G	X
case #7	25G	1G	10G	25G	X

Note

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

N3224F-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 1G SFP port	(8) 10G SFP+	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) HiGig2 stacking ports (QSFP28)

Switch System Characteristics

Mechanical Dimension	Standard 1U chassis height
Management-ethernet port	1
Console port	1
1G SFP port	24
10G SFP+ port	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
1G SFP port LED	1 x 24
10G SFP+ port LED	2 x 4
HiGig2 stacking ports (QSFP28)	2
HiGig2 stacking ports (QSFP28) LED	4 x 2
Micro-USB	1
USB port	1

Reset button	1
PSU	2
FAN	3

HiGig2 Stacking Ports

HiGig2 stacking ports at the rear side can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are x-1/1/1 and xe-1/1/2. They can be used as normal 100G QSFP28 ports.

Z9100-ON

Front Panel Schematic

(1) System Status LED	(2) Power Status LED	(3) FAN Status LED
(4) System Beacon LED	(5) Platform Stacking LED	(6) QSFP28 port
(7) SFP+ port	(8) USB port	(9) Management Ethernet port
(10) RJ45 Console port	(11) Micro-USB port	(12) 7-DIGIT Stack LED
(13) Reset button	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) PSU5	-	-

Switch System Characteristics

Mechanical dimension	Standard 1U chassis high
Management port	1
RJ45 Console port	1
QSFP28 port	32
SFP+ port	2
7-DIGIT Stack LED	1
System Status LED	1
Power Status LED	1
FAN Status LED	1
Status LED	1
System Beacon LED	1
Platform Stacking LED	1
USB port	1
Reset button	1

PSU	2
FRU(Fan Removable Unit)	5
Working environment temperature	0ºC～75ºC

N2248X-ON/N2248PX-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 1GbE/2.5GbE port	(8) 25GbE SFP28	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(5) 40GbE QSFP

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
1GbE/2.5GbE port	48
25GbE SFP28	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
RJ45 port LED	1 x 48
25GbE SFP28 LED	2 x 4
40GbE QSFP	2
40GbE QSFP LED	2 x 2
Micro-USB	1
USB port	1

Reset button	1
PSU	2
FAN	3

***UPoE**

The last 24 RJ45 ports on the front panel of N2248PX-ON support UPoE, the maximum output power can be set to up to 60 watts. The first 24 RJ45 ports support PoE but not UPOE, the maximum output power can be set to up to 30 watts.

25GbE SFP28 Port

Ports te-1/1/1, te-1/1/2, te-1/1/3 and te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the set interface gigabit-ethernet speed command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	X
case #6	25G	10G	25G	10G	X
case #7	25G	1G	10G	25G	X

Note:

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

N3208PX-ON

Front Panel Schematic

(1) System Status LED	(2) Power Status LED	(3) FAN Status LED
(4) System Beacon LED	(5) Console port	(6) Management Ethernet port
(7) 4 x 1G RJ45 ports	(8) 4x5G RJ45 ports	(9) 2x10G SPF+ ports
(10) USB port	(11) Reset button	-

Rear Panel Schematic

(1) PSU1	(2) FAN1	-

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height
Management port	1
RJ45 Console port	1
1G RJ45 port	4
5G RJ45 port	4
10G SPF+ port	2
Power LED	1
System Status LED	1
FAN Status LED	1
System Beacon LED	1
USB port	1
Reset button	1
PSU	1
FRU (Fan Removable Unit)	1
Working environment temperature	0ºC～70ºC

***UPoE**

- The first eight RJ45 ports, from ge-1/1/1 to ge-1/1/8, on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts. For details about UPoE, please refer to UPoE.
- See the link PoE Configuration Commands for PoE command reference, the following two PoE commands are not supported on N3208PX-ON:

set poe interface {<*interface-name*> | **all**} **max-power** <*integer*>

set poe power management-mode <*value*>

1G/2.5G/5G RJ45 Port

The four 1G/2.5G/5G RJ45 ports, ge-1/1/5, ge-1/1/6, ge-1/1/7 and ge-1/1/8, don't support setting of the force speed by using **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command, but only supports auto-negotiation mode. Together with the optional **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** <*auto-speed*> command, user can manually specify the auto-negotiation rate range.

N3224P-ON//N3224T-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 1G Cu port	(8) 10G SFP28 port	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) HiGig2 stacking ports (QSFP28)

Switch System Characteristics

Mechanical Dimension	Standard 1U chassis height
Management-ethernet port	1
Console port	1
1G Cu port	24
10G SFP28 port	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
1G Cu port LED	1 x 24
10G SFP28 port LED	2 x 4
HiGig2 stacking ports (QSFP28)	2
HiGig2 stacking ports (QSFP28) LED	4 x 2
Micro-USB	1
USB port	1

Reset button	1
PSU	2
FAN	3

***PoE**

- The 24 RJ45 ports on the front panel of N3224P-ON support PoE but N3224T-ON doesn't support. For these PoE ports, the maximum output power can be set to up to 30 watts.
- See the link PoE Configuration for PoE command reference,.

Notes:

The following PoE commands are not supported on N3224P-ON:

- **set poe interface max-power**
- **set poe interface detection-type**
- **set poe interface mode**
- **set poe interface threshold-mode**
- **set poe power management-mode**

25GbE SFP28 Port

Ports Te-1/1/25, Te-1/1/26, Te-1/1/27 and Te-1/1/28 are a group of ports, you should manually configure the port speed for these four ports by using the set interface gigabit-ethernet speed command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/25	**te-1/1/26**	**te-1/1/27**	**te-1/1/28**	**Allowed or not allowed**
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	X
case #6	25G	10G	25G	10G	X
case #7	25G	1G	10G	25G	X

Note

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

HiGig2 stacking ports

N3224P-ON has one slot for QSFP module at the rear side which can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are x-1/1/1 and xe-1/1/2. They can be used as normal 100G QSFP28 ports.

N3224PX-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 10G Cu port	(8) 25GbE SFP28	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) HiGig2 stacking ports (QSFP28)

Switch System Characteristics

Mechanical Dimension	Standard 1U chassis height
Management-ethernet port	1
Console port	1
10G Cu port	24
25GbE SFP28	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
10G Cu port LED	1 x 24
25GbE SFP28 LED	2 x 4
HiGig2 stacking ports (QSFP28)	2
HiGig2 stacking ports (QSFP28) LED	4 x 2
Micro-USB	1
USB port	1

Reset button	1
PSU	2
FAN	3

***UPoE**

- The 24 RJ45 ports on the front panel of N3224PX-ON support UPoE. For these UPoE ports, the maximum output power can be set to up to 99 watts. For details about UPoE, please refer to UPoE.
- See the link PoE Configuration Commands for PoE command reference.

Note:

The following PoE commands are not supported on N3224PX-ON:

set poe interface max-power

set poe interface mode

set poe interface threshold-mode

set poe power management-mode

25GbE SFP28 Port

Ports Te-1/1/25, Te-1/1/26, Te-1/1/27 and Te-1/1/28 are a group of ports, you should manually configure the port speed for these four ports by using the set interface gigabit-ethernet speed command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/25	te-1/1/26	te-1/1/27	te-1/1/28	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	X
case #6	25G	10G	25G	10G	X
case #7	25G	1G	10G	25G	X

Note:

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

HiGig2 stacking ports

N3224PX-ON has one slot for QSFP module at the rear side which can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are x-1/1/1 and xe-1/1/2. They can be used as normal 100G QSFP28 ports.

N3248P-ON/N3248TE-ON

Front Panel Schematic

(1) Platform Stacking LED	(2) System Status LED	(3) Power Status LED
(4) FAN Status LED	(5) System Beacon LED	(6) 7-Digit Stacking LED
(7) 48 x 1G RJ45 ports	(8) 4x10G SFP+ ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) 2 x QSFP28 ports

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height
Management port	1
RJ45 Console port	1
1G RJ45 port	48
10G SFP28 port	4
QSFP28 ports	2
7-DIGIT Stack LED	1
Power LED	1
System Status LED	1
Platform Stacking LED	1
FAN Status LED	1
USB port	1
Reset button	1
PSU	2
FRU (Fan Removable Unit)	3
Working environment temperature	0ºC ~ 75ºC

***PoE**

The 48x1G RJ45 ports on the front panel of N3248P-ON support PoE, but N3248TE-ON doesn't support PoE, the maximum output power supported is up to 30 watts. See the link PoE Configuration Commands for PoE command reference.

Notes:

The following PoE commands are not supported on N3248P-ON:

- **set poe interface max-power**
- **set poe interface mode**
- **set poe interface threshold-mode**
- **set poe power management-mode**

1G RJ45 Port

The 10/100/1000M RJ45 ports don't support setting of the force speed by using **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command, but only supports auto-negotiation mode. Together with the optional **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** <*auto-speed*> command, user can manually specify the auto-negotiation rate range.

25GbE SFP28 Port

Ports Te-1/1/1, Te-1/1/2, Te-1/1/3 and Te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note:

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

HiGig2 stacking ports

N3248P-ON has one slot for QSFP module at the rear side which can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are Xe-1/1/1 and Xe-1/1/2. They can be used as normal 100G QSFP28 ports.

N3248PXE-ON/N3248X-ON

Front Panel Schematic

(1) Platform Stacking LED	(2) System Status LED	(3) Power Status LED
(4) FAN Status LED	(5) System Beacon LED	(6) 7-Digit Stacking LED
(7) 48 x 2.5G/5G RJ45 ports	(8) 4x25G SFP28 ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button

Rear Panel Schematic

(1) PSU(Power Supply Unit)	(2) PSU LED	(3) FAN1
(4) FAN2	(5) FAN3	(6) 2xHG[106] stacking ports

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height
Management port	1
RJ45 Console port	1
2.5G/5G RJ45 port	48
25G SFP28 port	4
HG[106] stacking ports	2
7-DIGIT Stack LED	1
Power LED	1
System Status LED	1
Platform Stacking LED	1
FAN Status LED	1
USB port	1
Reset button	1
PSU	2
FRU(Fan Removable Unit)	3
Working environment temperature	0ºC ~ 75ºC

***UPoE**

- The 48x10G RJ45 ports on the front panel of N3248PXE-ON support UPoE. For these UPoE ports, the maximum output power supported is up to 99 watts. For details about UPoE, please refer to UPoE.
- N3248X-ON does not support PoE.
- See the link PoE Configuration Commands for PoE command reference.

Notes:

The following PoE commands are not supported on N3248PXE-ON:

- **set poe interface max-power**
- **set poe interface mode**
- **set poe interface threshold-mode**
- **set poe power management-mode**

2.5G/5G RJ45 Port

The 2.5G/5G RJ45 ports don't support setting of the force speed by using **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command, but only supports auto-negotiation mode. Together with the optional **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** <*auto-speed*> command, user can manually specify the auto-negotiation rate range. The supported speeds include **10M, 100M**, **1G**, **2.5G**, **5G** and **10G**.

25GbE SFP28 Port

Ports Te-1 / 1/49, Te-1 / 1/50, Te-1 / 1/51 and Te-1 / 1/52 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/49	te-1/1/50	te-1/1/51	te-1/1/52	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note:

If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

2 x HG[106] stacking ports

N3248PXE-ON/N3248X-ON has one slot for QSFP module at the rear side which can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are Xe-1/1/1 and Xe-1/1/2. They can be used as normal 100G QSFP28 ports.

N3248TE-ON

Front Panel Schematic

(1) Platform Stacking LED	(2) System Status LED	(3) Power Status LED
(4) FAN Status LED	(5) System Beacon LED	(6) 7-Digit Stacking LED
(7) 48 x 1G RJ45 ports	(8) 4x10G SFP+ ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) 2 x 100G QSFP28 ports

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height
Management port	1
RJ45 Console port	1
1G RJ45 port	48
10G SFP28 port	4
QSFP28 ports	2
7-DIGIT Stack LED	1
Power LED	1
System Status LED	1
Platform Stacking LED	1
FAN Status LED	1
USB port	1
Reset button	1
PSU	2
FRU (Fan Removable Unit)	3
Working environment temperature	0ºC ~ 75ºC

QSFP28 ports

N3248TE-ON has one slot for QSFP module at the rear side which can be plugged in 2 x 100G QSFP modules. The port numbers of the QSFP module are xe-1/1/1 and xe-1/1/2. They can be used as normal 100G QSFP28 ports.

S4048

Front Panel Schematic

(1) Power Status LED	(2) PSU LED	(3) FAN Status LED
(4) Master LED	(5) Located LED	(6) 7-Digit Stacking LED
(7) Health LED	(8) 48 x 10G SFP+ ports	(9) 6x40G QSFP+ ports
(10) Console port	(11) Management Ethernet port	(12) Reset button
(13) USB port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height
Management port	1
RJ45 Console port	1
10G SFP+ ports	48
40G QSFP+ ports	6
HiGig2 stacking ports	2
Power Status LED	1
PSU LED	1
Master LED	1
Located LED	1
FAN Status LED	1
7-Digit Stacking LED	1
USB port	1
Reset button	1
PSU	2
FRU (Fan Removable Unit)	6

Working environment temperature	0ºC ~ 75ºC

S4128F-ON/S4128T-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
*(7) 10G SFP+ port /10GBT RJ45 port	(8) 100G QSFP28 port	(9) USB port
(10) Micro-USB port	-	-

Rear Panel Schematic

(1) PSU(Power Supply Unit)	(2) PSU LED	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) RJ45 Console port	(8) Management Ethernet port	-

Switch System Characteristics

Mechanical dimension	Standard 1U chassis high
Management port	1
RJ45 Console port	1
10G SFP+ port	28
100G QSFP28 port	2
7-DIGIT Stack LED	1
Stacking LED	1
System LED	1
Power LED	1
FAN LED	1
USB port	1
Micro-USB port	1
PSU	2
FRU(Fan Removable Unit)	4
Working environment temperature	0ºC～75ºC

*** 10G SFP+ port /10GBT RJ45 port**

On S4128T-ON, the 28 x 10G ports on the front panel, Te-1/1/1 to Te-1/1/24 and Te-1/1/27 to Te-1/1/30, are 10GBT RJ45 ports. However, on S4128F-ON, they are 10G SFP+ ports.

S4148T-ON/S4148F-ON

Front Panel Schematic

(1) Stacking LED	(2) System LED	(3) Power LED
(4) FAN LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
*(7) 10GBT RJ45 port/10G SFP+ port	(8) 40G QSFP+ port	(9) 100G QSFP28 port
(10) USB port	(11) Micro-USB port	-

Rear Panel Schematic

(1) PSU(Power Supply Unit)	(2) PSU LED	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) RJ45 Console port	(8) Management Ethernet port	

Switch System Characteristics

Mechanical dimension	Standard 1U chassis high
Management port	1
RJ45 Console port	1
*10GBT RJ45 port/10G SFP+ port	48
40G QSFP+ port	2
100G QSFP28 port	4
7-DIGIT Stack LED	1
Stacking LED	1
System LED	1
Power LED	1
FAN LED	1
USB port	1
Micro-USB port	1
PSU	2
FRU(Fan Removable Unit)	4
Working environment temperature	0ºC～75ºC

*** 10GBT RJ45 port/10G SFP+ port**

On S4148T-ON, the 48 x 10G ports on the front panel, Te-1/1/1 to Te-1/1/24 and Te-1/1/31 to Te-1/1/54, are 10GBT RJ45 ports. However, on S4148F-ON, they are 10G SFP+ ports.

S5212F-ON

Front Panel Schematic

(1) Platform Stacking LED	(2) System Status LED	(3) System Beacon LED
(4) Power Status LED	(5) FAN Status LED	(6) 7-Digit Stacking LED
(7) 12x25G SFP ports	(8) 3x100G QSFP28 ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button
(13) PSU(Power Supply Unit)	(14) PSU LED	-

Rear Panel Schematic

(1) FAN1	(2) FAN2	(3) FAN3
(4) FAN4	-	-

Switch System Characteristics

Mechanical dimension	Standard 1U chassis height, half-rack width
Management port	1
RJ45 Console port	1
25G SFP28 port	12
100G QSFP28 port	3
7-DIGIT Stack LED	1
Power LED	1
System Status LED	1
Platform Stacking LED	1
FAN Status LED	1
USB port	1
Reset button	1
PSU	2
FRU(Fan Removable Unit)	4
Working environment temperature	0ºC～75ºC

S5224F-ON

NOTE:

When the system is running normally, if one of the four fans or one of the two power supply units is removed, the remaining fans will run at a full speed. The fan fault alarm is reported and the fan LED changes to solid amber. Until the fan is reinserted, the fan fault recovers, and the system restarts adjusting the fan speed intelligently to control the device temperature within a reasonable range.

Front Panel Schematic

(1) Power LED	(2) Stacking LED	(3) FAN LED
(4) System LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 25GbE SFP28 port	(8) 100GbE QSFP28 port	(9) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) Management Ethernet port	Console port	(9) USB port
(10) Micro USB	-	-

Switch System Characteristics

Mechanical Dimension	Standard 1RU form factor
Management-ethernet port	1
Console port	1
25G SFP28 port	48
100G QSFP28 port	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
25G SFP28 port LED	48

100G QSFP28 port LED	4 x 4
Micro-USB	1
USB port	1
Reset button	1
PSU	2
FAN	4

S5232F-ON

Front Panel Schematic

(1) Power LED	(2) Stacking LED	(3) FAN LED
(4) System LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7)100GbE QSFP28 port	(8) 10GbE SFP+ port	(9) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) Management Ethernet port	(8) Console port	(9) USB port
(10) Micro USB	-	-

Switch System Characteristics

Mechanical Dimension	Standard 1RU form factor
Management-ethernet port	1
Console port	1
100GbE QSFP28 port	32
10GbE SFP+ port	2
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
100GbE QSFP28 port LED	4 x 32
10G SFP+ port LED	4
Micro-USB	1
USB port	1
Reset button	1
PSU	2

FAN	4

S5248F-ON

Front Panel Schematic

(1) Power LED	(2) Stacking LED	(3) FAN LED
(4) System LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 25G SFP28 port	(8) QSFP-DD port	(9) 100G QSFP28 port
(10) Reset button	(11) Micro-USB	(12) USB port
(13) Management Ethernet port	(14) Console port	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical Dimension	Standard 1RU form factor
Management-ethernet port	1
Console port	1
25G SFP28 port	48
QSFP-DD port	2
100G QSFP28 port	4
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
25G SFP28 port	48
QSFP-DD port LED	2 x 8
100G QSFP28 port LED	4 x 4
Micro-USB	1
USB port	1

Reset button	1
PSU	2
FAN	4

S5296F-ON

Front Panel Schematic

(1) Power LED	(2) Stacking LED	(3) FAN LED
(4) System LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) 25G SFP28 port	(8) 100G QSFP28 port	(9) Reset button
(10) Micro-USB	(11) USB port	(12) Console port
(13) Management Ethernet port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical Dimension	446 mm (L: Length) x 515mm (D: Depth) x 86 mm (H: Height maximum)
Management-ethernet port	1
Console port	1
25G SFP28 port	96
100G QSFP28 port	8
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
25G SFP28 port LED	1 x 96
100G QSFP28 port	4 x 8
Micro-USB	1
USB port	1
Reset button	1
PSU	2

FAN	4

Z9264F-ON

Front Panel Schematic

(1) Power LED	(2) Stacking LED	(3) FAN LED
(4) System LED	(5) Beacon LED	(6) 7-DIGIT Stack LED
(7) QSFP28 port	(8) SFP+ port	(9) QSFP28 port LED
(10) SFP+ port LED	(11) Micro-USB	(12) USB port
(13) Management Ethernet port	(14) Console port	(15) Reset button
(16) ESD jack	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical Dimension	442 mm (L: Depth) x 510mm (W: Width) x 85.6 mm (H: Height maximum)
Management-ethernet port	1
Console port	1
QSFP28 port	64
SFP+port	2
Power LED	1
Stacking LED	1
FAN LED	1
System LED	1
Beacon LED	1
7-DIGIT Stack LED	1
SFP+ port LED	2
QSFP28 port LED	4 x 64
Micro-USB	1
USB port	1
Reset button	1

PSU	2
FAN	4
Operation temperature	0ºC ~ 85ºC

EdgeCore/Accton

- AS7816-64X
- AS5835_54X
- AS9716-32D
- AS4610-30P
- AS4610-30T
- AS4610-54P
- AS4610-54T
- AS4625-54P/AS4625-54T
- AS4630-54NPE
- AS4630-54PE
- AS5712_54X/HP5712
- AS5812_54T
- AS5812_54X
- AS5835_54T
- AS6812_32X
- AS7312_54X / AS7312_54XS
- AS7326-56X
- AS7712-32X
- AS7726-32X

AS7816-64X

Front Panel Schematic

(1) Location LED	(2) Diagnosis LED	(3) FAN Status LED
(4) PSU1 LED	(5) PSU1 LED	(6) QSFP28 ports
(7) RJ45 Console port	(8) Management Ethernet port	(9) USB port
(10)Reset button	-	-

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical dimension	2U high chassis: 580 mm (L: Depth) x 438.4mm (W: Width) x 88 mm (H: Height maximum)
Management port	1
RJ45 Console port	1
QSFP28 ports	64
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	3+1
Working environment temperature	0ºC ~ 45ºC

AS5835_54X

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

AS9716-32D

Front Panel Schematic

(1) Locator LED	(2) Diagnosis LED	(3) FAN Status LED
(4) PS1 LED	(5) PS2 LED	(6) SFP+ 10G management ports
(7) RJ45 10/100/1G Management port	(8) RJ45 Console port	(9) QSFP56-DD 400G ports
(10) Reset button	(11) USB port	(12) PTP Clock output

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	Height: 43.1mm (maximum), Width: 438.4mm, Depth: 536mm
SFP+ 10G management port	2
SFP+ 10G management port LED	1 x 2
RJ45 10/100/1G Management port	1
RJ45 Console port	1
QSFP56-DD 400G port	32
QSFP56-DD 400G port LED	4 x 32
Locator LED	1
Diagnosis LED	1
FAN Status LED	1
PS1 LED	1
PS2 LED	1
PS	1+1
FAN	5+1
Working environment temperature	0 to +45 Degree C

AS4610-30P

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7) PRI LED	(8) PoE LED	(9) Reset button
(10) 1GbE RJ45 port	(11) 10GbE SFP+ port	(12) 40GbE QSFP port
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	24
10G SFP+	4
40G QSFP	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1
PSU	2
FAN	1

***UPoE**

- Only the last 8 RJ45 ports of the switch, which are, ge-1/1/17 - ge-1/1/24 on AS4610-30P support UPoE, other ports support PoE.

- For UPoE ports the range is from 1W to 51W, for other ports the range is from 1W to 32W. The default value is 16W.

AS4610-30T

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) PRI LED	(5) PSU2 LED	(6) STK2 LED
(7) 1GbE RJ45 port	(8) 10GbE SFP+ port	(9) 40GbE QSFP port
(10) Management Ethernet port	(11) Console port	(12) Reset button
(13) USB port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	24
10G SFP+	4
40G QSFP	2
PSU LED	2
STK LED	2
System LED	1
PRI LED	1
USB port	1
Reset button	1
PSU	2

AS4610-54P

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7) PRI LED	(8) PoE LED	(9) Reset button
(10) 1GbE RJ45 port	(11) 10GbE SFP+ port	(12) 40GbE QSFP port
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	48
10G SFP+	4
40G QSFP	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1
PSU	2
FAN	1

***UPoE**

- Only the last 8 RJ45 ports of the switch, which are, ge-1/1/41 -- ge-1/1/48 on AS4610-54P support UPoE, other ports support PoE.

- For UPoE ports the range is from 1W to 51W, for other ports the range is from 1W to 32W. The default value is 16W.

AS4610-54T

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) PRI LED	(5) PSU2 LED	(6) STK2 LED
(7) 1GbE RJ45 port	(8) 10GbE SFP+ port	(9) 40GbE QSFP port
(10) Management Ethernet port	(11) Console port	(12) Reset button
(13) USB port	-	-

Rear Panel Schematic

(1) PSU1	(2) PSU2	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	48
10G SFP+	4
40G QSFP	2
PSU LED	2
STK LED	2
System LED	1
PRI LED	1
USB port	1
Reset button	1
PSU	2

AS4625-54P/AS4625-54T

Front Panel Schematic

(1) System Status LED	(2) PSU1 LED	(3) FAN Status LED
(4) Location LED	(5) PSU2 LED	(6) PoE Status LED (Only for AS4625-54P)
(7) 48 x 1G RJ45 ports	(8) 6 x10G SFP+ ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical dimension	350.35mm (L: Depth) x 440mm (W: Width) x 44mm (H: Height)
Management port	1
RJ45 Console port	1
1G RJ45 port	48
10G SFP+ port	6
System Status LED	1
PSU1 LED	1
PSU2 LED	1
FAN Status LED	1
Location LED	1
PoE Status LED (Only for AS4625-54P)	1
USB port	1
Reset button	1
PSU	2
FRU (Fan Removable Unit)	3
Operating environment temperature	0ºC～45ºC

***PoE (Only for AS4625-54P)**

The 48 x 1G RJ45 ports on the front panel support PoE. Port1~Port40 support supports IEEE802.3at/af, the maximum output power supported is up to 30 watts, Port41~Port48 support IEEE802.3bt standard, the maximum output power supported is up to 90 watts.

AS4630-54NPE

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7) PRI LED	(8) PoE LED	(9) Reset button
(10) RJ45 port	(11) 25GbE SFP28	(12) 100GbE QSFP28
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
2.5G Base-T	36
10G Base-T	12
25G SFP28	4
100G QSFP28	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1
PSU	2
FAN	3

***UPoE**

The first 48 RJ45 ports on the front panel of AS4630-54NPE support UPoE, the maximum output power can be set to up to 90 watts, the default value is 30 watts.

AS4630-54PE

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7)PRI LED	(8) PoE LED	(9) Reset button
(10) RJ45 port	(11) 25GbE SFP28	(12) 100GbE QSFP28
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	48
25G SFP28	4
100G QSFP28	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1
PSU	2
FAN	3

***UPoE**

The first 48 RJ45 ports on the front panel of AS4630-54PE support UPoE, the maximum output power can be set to up to 90 watts, the default value is 30 watts.

AS5712_54X/HP5712

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5		

AS5812_54T

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) RJ45 port	(8) QSFP+ port LED	(9) RJ45 port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

AS5812_54X

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5		

AS5835_54T

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP 28 port
(7) RJ45 port	(8) QSFP 28 port LED	(9) RJ45 port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

AS6812_32X

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 40G QSFP port
(7) Management Ethernet port	(8) RJ45 Console port	(9) Reset button

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

Switch System Characteristics

Mechanical dimension	515 mm (L: Depth) x 438.4mm (W: Width) x 44 mm (H: Height)
Management port	1
RJ45 Console port	1
40G QSFP port	32
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
PSU	1+1
FAN	5
Working environment temperature	0 to +40 Degree C

AS7312_54X / AS7312_54XS

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port
(13) Reset button		

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	

Switch System Characteristics

Mechanical Dimension	515 mm (L: Depth) x 438.4mm (W: Width) x 43.5 mm (H: Height maximum)
Management-ethernet port	1
Console port	1
SFP+port	48
QSFP+port	6
PS1 LED	1
PS2 LED	1
FAN LED	1
Diag LED	1
LOC LED	1
SFP+port LED	48
QSFP+port LED	6
Reset button	1
RPSU	2
FRU	6

Working environment temperature	0ºC～45ºC

AS7326-56X

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 25G SFP28 port
(7)100G QSFP28 port	(8)10G SFP+ port	(9) Management Ethernet port
(10) RJ45 Console port	(11) USB port	(12)Reset button

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	

Switch System Characteristics

Mechanical dimension	1U high and 536mm deep chassis
Management port	1
RJ45 Console port	1
25G SFP28 port	48
100G QSFP28 port	8
10G SFP+ port	2
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	6
Working environment temperature	0 to +40 Degree C

AS7712-32X

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 100G QSFP28 port
(7) USB port	(8) RJ45 Console port	(9) Management Ethernet port
(10) Reset button	-	-

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	1U high and 515mm deep
Management port	1
RJ45 Console port	1
100G QSFP28 port	32
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	6
Working environment temperature	0ºC～45ºC

AS7726-32X

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 100G QSFP28 port
(7)10G SFP+ port	(8) RJ45 Console port	(9) Management Ethernet port
(10) USB port	(11)Reset button	-

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	1U high and 515mm deep
Management port	1
RJ45 Console port	1
100G QSFP28 port	32
10G SFP+ port	2
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	6
Working environment temperature	0ºC～45ºC

Delta/Agema

- AG9032v1
- AG5648V1
- AG7648

AG9032v1

Front Panel Schematic

(1) Power 1 LED	(2) Power 1 LED	(3) System LED
(4) FAN Status LED	(5) QSFP+ port	(6) USB port
(7) Management port	(8) Console port	(9) Reset button

Rear Panel Schematic

(1) PSU	(2) PSU LED	(3) FAN Status LED
(4) FAN1	(5) FAN2	(6) FAN3
(7) FAN4	(8) FAN5	-

Switch System Characteristics

Mechanical Dimension	Standard 1U chassis high
Management port	1
Console port	1
QSFP+port	32
Power 1 LED	1
Power 2 LED	1
System LED	1
FAN Status LED	1
Reset button	1
PSU	2
FRU	5
Working environment temperature	0ºC～45ºC

AG5648V1

Front Panel Schematic

(1) Power LED	(2) System LED	(3) FAN LED
(4) QSFP28 port	(5) SFP28 port	(6) QSFP28 port LED
(7) SFP28 port LED	(8) Management Ethernet port	(9) Console port
(10) USB port	(11) Reset button	-

Rear Panel Schematic

(1) PSU1 (removable power supply unit)	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical Dimension	Standard 1U chassis high
Management-ethernet port	1
Console port	1
SFP28 port	48
QSFP28 port	6
Power LED	1
FAN LED	1
System LED	1
SFP28 port LED	48
QSFP28 port LED	6
Reset button	1
PSU	2
FRU	4
Working environment temperature	0ºC ~ 70ºC

AG7648

Front Panel Schematic

(1) FAN Status LED	(2) Power LED	(3) System LED
(4) Locator LED	(5) 10G SFP+ port	(6) 40G QSFP+ port
(7) RJ45 Console port	(8) RJ45 Console port	(9) USB port

Rear Panel Schematic

(1) PSU1 (Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) Management port
(7) PSU LED	(8) -	(9) -

Switch System Characteristics

Mechanical dimension	Standard 1U chassis high
Management port	1
RJ45 Console port	1
10G SFP+ port	48
40G QSFP+ port	6
Locator LED	1
System LED	1
FAN Status LED	1
PSU LED	1
PSU	1+1
FAN	3
Working environment temperature	0 to +40 Degree C

FS

- N8550-48B8C
- S5810-48TS-P
- S5810-28FS
- S5810-28TS
- S5810-48FS
- S5810-48TS
- S5860-20SQ
- S5860-24XB-U
- N8560-32C
- N8560-64C
- S5860-24MG-U
- S5860-48XMG-U
- S5860-48XMG
- S5860-24XMG
- S5860-48MG-U
- S5870-48T6S/S5870-48T6S-U
- S5870-48T6BC/S5870-48T6BC-U
- N5850-48X6C
- N8550-64C
- N9550-32D
- N5850-48S6C
- S5870-48MX6BC-U
- S3410-24TS
- S3410L-24TF
- S3410L-24TF-P
- S3410-24TS-P
- N8550-32C
- S3410C-8TMS-P
- S3410C-16TF
- N5850-48S6Q
- S3410C-16TMS-P
- S3410C-16TF-P
- S3410-48TS-P
- S3410-48TS
- S3410L-48TF
- N8550-24CD8D
- N9600-64OD

N8550-48B8C

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 25G SFP28 port
(7)100G QSFP28 port	(8)10G SFP+ port	(9) Management Ethernet port
(10) RJ45 Console port	(11) USB port	(12)Reset button

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	

Switch System Characteristics

Mechanical dimension	1U high and 536mm deep chassis
Management port	1
RJ45 Console port	1
25G SFP28 port	48
100G QSFP28 port	8
10G SFP+ port	2
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	6
Working environment temperature	0 to +40 Degree C

S5810-48TS-P

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) MGMT LED	(5) PoE LED	(6) PoE Button
(7) RJ45 Management port	(8) Console port	(9) Mini Console port
(10) 10/100/1000BASE-T RJ45 port	(11) SFP+ 10G port	(12) USB port

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.73"x17.32"x16.54" (44x440x420mm), 1 U
SFP+ 10G management port	2
SFP+ 10G management port LED	1 x 2
RJ45 Management port	1
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	48
10/100/1000BASE-T RJ45 port LED	48
SFP+ 10G port	4
SFP+ 10G LED	4
Status LED	1
PWR1 LED	1
PWR2 LED	1
MGMT LED	1
PoE LED	1
PoE button	1
Power Supply	1+1
FAN	3 x Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

NOTE

PoE button:

The 48x1G RJ45 ports on the front panel support PoE, the maximum output power supported is up to 30 watts.

PoE button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 48 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

S5810-28FS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) MGMT LED	(5) RJ45 Management port	(6) Console port
(7) Mini Console port	(8) USB port	(9) GE RJ45 port (Combo)
(10) GE SFP port	(11) 10GE SFP+ port	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (WxDxH)	440×280×44mm
RJ45 Management port	1
Console port	1
10/100/1000BASE-T RJ45 port (Combo)	8
10/100/1000BASE-T RJ45 port LED	8 x 1
GE SFP port	28
GE SFP port LED	28 x 1
10G SFP+ port	4
10G SFP+ LED	4 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
MGMT LED	1
Mini Console port	1
USB port	1
Power Supply	1+1
FAN	3 x Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

NOTE

Combo Port

1. Ports Ge-1/1/1, Ge-1/1/2, Ge-1/1/3, Ge-1/1/4, Ge-1/1/5, Ge-1/1/6, Ge-1/1/7 and Ge-1/1/8 are combo ports that support maximum of 1G port speed. A combo port consists of a GE electrical interface and a GE optical interface separately on the front panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled.

   The electrical port has a higher priority, that is, as long as the electrical port is plugged in, the electrical port takes effect but the optical port is invalid.

2. When configuring port speed, the combo ports (when worked as electrical ports) only support auto-negotiation mode, that is, configuring the force rate will not take effect for combo port when it works as an electrical port.

S5810-28TS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) MGMT LED	(5) RJ45 Management port	(6) Console port
(7) Mini Console port	(8) USB port	(9) GE RJ45 port
(10) GE SFP port (Combo)	(11) 10GE SFP+ port	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (WxDxH)	440 X 280 X 44mm
RJ45 Management port	1
Console port	1
10/100/1000BASE-T RJ45 port	28
10/100/1000BASE-T RJ45 port LED	28 x 1
GE SFP port (Combo)	4
GE SFP port LED	4 x 1
10G SFP+ port	4
10G SFP+ LED	4 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
MGMT LED	1
Mini Console port	1
USB port	1
Power Supply	1+1
FAN	3 x Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

NOTE

Combo Port

1. Ge-1/1/25, Ge-1/1/26, Ge-1/1/27 and Ge-1/1/28 ports are combo ports that support 1G port speed. A combo port consists of a GE electrical interface and a GE optical interface separately on the front panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled.

   The electrical port has a higher priority, that is, as long as the electrical port is plugged in, the electrical port takes effect but the optical port is invalid.

2. When configuring port speed, the combo ports (when worked as electrical ports) only support auto-negotiation mode, that is, configuring the force rate will not take effect for combo port when it works as an electrical port.

S5810-48FS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) MGMT LED	(5) RJ45 Management port	(6) Console port
(7) Mini Console port	(8) USB port	(9) GE SFP port
(10) 10G SFP+ port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.73"x17.32"x16.54" (44x440x420mm), 1 U
RJ45 Management port	1
RJ45 Console port	1
GE SFP port	48
GE SFP port LED	48
10G SFP+ port	4
10G SFP+ LED	4
Status LED	1
PWR1 LED	1
PWR2 LED	1
MGMT LED	1
Power Supply	1+1
FAN	3 Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

S5810-48TS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) MGMT LED	(5) RJ45 Management port	(6) Console port
(7) Mini Console port	(8) USB port	(9) 10/100/1000BASE-T RJ45 port
(10) SFP+ 10G port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.73"x17.32"x16.54" (44x440x420mm), 1 U
RJ45 Management port	1
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	48
10/100/1000BASE-T RJ45 port LED	48
SFP+ 10G port	4
SFP+ 10G LED	4
Status LED	1
PWR1 LED	1
PWR2 LED	1
MGMT LED	1
Power Supply	1+1
FAN	3 x Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

S5860-20SQ

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) FAN Status LED	(5) MGMT LED	(6) ID LED
(7) RJ45 Management port	(8) RS232 Console port	(9) SFP+ 10G port
(10) SFP28 25G port	(11) QSFP+ 40G port	(12) FUNC button (Reset button)
(13) USB port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	-	-

Switch System Characteristics

Mechanical dimension	442 mm × 330 mm × 43.6 mm (17.40 in. x 12.99 in. x 1.72 in.), 1 RU
RJ45 1G Management port	1
RS232 Console port	1
SFP+ 10G port	20
SFP+ 10G port LED	20 x 1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
QSFP+ 40G port	2
QSFP+ 40G port LED	2 x 4
Status LED	1
PWR1 LED	1
PWR2 LED	1
FAN Status LED	1
MGMT LED	1
ID LED	1
FUNC button	1 (the reset button)
Power Supply	1+1

FAN	2
Working environment temperature	0°C to 50°C (32°F to 122°F)

S5860-24XB-U

Front Panel Schematic

(1) System LED	(2) PWR LED	(3) FAN LED
(4) PoE LED	(5) MGMT LED	(6) RJ45 Management port
(7) RS232 Console port	(8) FUNC button (Reset button)	(9) USB port
(10) PoE button	(11) RJ45 10G port	(12) SFP+ 10G port
(13) SFP28 25G port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical dimension	442 mm × 330 mm × 43.6 mm (17.40 in. x 12.99 in. x 1.72 in.), 1 RU
RJ45 10G port	24
RJ45 10G port LED	24 x 1
RJ45 10/100/1G Management port	1
RJ45 Console port	1
SFP+ 10G port	4
SFP+ 10G port LED	4 x 1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
System LED	1
PWR LED	1
FAN LED	1
MGMT LED	1
FUNC button	1 (reset button)
Power Supply	1+1
FAN	2+1

Working environment temperature	0°C to 50°C (32°F to 122°F)

NOTE

*UPoE and PoE button

The first 24 x10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts.

PoE button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 24 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

N8560-32C

Front Panel Schematic

(1) System LED	(2) PSU LED	(3) FAN LED
(4) USB port	(5) RJ45 Management port	(6) Console port
(7) 100G QSFP28 port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

Switch System Characteristics

Mechanical dimension (WxDxH)	442 mm x 560 mm x 44 mm (17.40 in. x 22.05 in. x 1.73 in., 1 RU)
RJ45 Management port	1
Console port	1
100G QSFP28 port	32
100G QSFP28 port LED	32
System LED	1
PSU LED	1
FAN LED	1
Power Supply	1+1
FAN	4+1
Working environment temperature	0°C to 40°C (32ºF to 104ºF)

N8560-64C

Front Panel Schematic

(1) BMC LED	(2) SYS LED	(3) PSU LED
(4) FAN LED	(5) LCT LED	(6) RJ45 Management port
(7) Console port	(8) USB port	(9) 40/100G QSPF28 port

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical dimension (WxDxH)	440mm x 580mm x 86mm
BMC LED	1
SYS LED	1
PSU LED (front panel)	1
FAN LED (front panel)	1
LCT LED	1
RJ45 Management port	1
Console port	1
USB port	1
40/100G QSPF28 port	64
40/100G QSPF28 port LED	64
Power Supply	1+1
FAN	2+1
PSU LED (rear panel)	2
FAN LED (rear panel)	3
Working environment temperature	0°C to 40°C (32ºF to 104ºF)

S5860-24MG-U

Front Panel Schematic

(1) Status LED	(2) MGMT LED	(3) LED Mode (LED)
(4) LED Mode (button)	(5) Console port	(6) RJ45 Management port
(7) USB port	(8) RJ45 5G port	(9) SFP28 25G port

Rear Panel Schematic

(1) PSU (Power Supply)	(2) FAN1 (at the right side of the switch)	(3) FAN2 (at the right side of the switch)

Switch System Characteristics

Mechanical dimension	220mm width, 1 U height
RJ45 5G port	24
RJ45 5G port LED	24 x 1
RJ45 10/100/1G Management port	1
Console port	1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
Status LED	1
MGMT LED	1
LED Mode (LED)	1
LED Mode (button)	1
Power Supply	1
FAN	2
Working environment temperature	0℃~45℃

NOTE

***PoE and LED Mode Button**

The first 24 RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts.

LED Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 24 ports.

- By default, port LED indicates data switching status of the port. LED Mode LED on the front panel of system LED block is solid green.
- If pressed the LED Mode button, the port LED indicates PoE power supply status of the port. LED Mode LED on the front panel of system LED block changes to solid amber.

S5860-48XMG-U

Front Panel Schematic

(1) Status LED	(2) MGMT LED	(3) PWR1 LED
(4) PWR2 LED	(5) FAN LED	(6) LED Mode (LED)
(7) LED Mode (button)	(8) RJ45 10G port	(9) SFP28 25G port
(10) QSFP+ 40G port	-	-

Rear Panel Schematic

(1) RJ45 Management port	(2) Console port	(3) USB port
(4) PS1 (Power Supply)	(5) PS2	(6) FAN1
(7) FAN2	(8) FAN3	-

Switch System Characteristics

Mechanical dimension (W x D x H)	442 mm x 420 mm x 43.6 mm (17.40 in. x 16.54 in. x 1.72 in.)
RJ45 10G port	48
RJ45 10G port LED	48 x 1
RJ45 10/100/1G Management port	1
Console port	1
USB port	1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
QSFP+ 40G port	2
QSFP+ 40G port LED	2 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
FAN LED	1
MGMT LED	1
LED Mode (LED)	1
LED Mode (button)	1

Power Supply	1+1
FAN	2+1
Working environment temperature	0°C to 45°C (32°F to 113°F)

NOTE

PoE and LED Mode Button

The first 48 x 10G RJ45 ports on the front panel support PoE, only the first 24 x 10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts. For other PoE ports, the maximum output power supported is 30 watts.

LED Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 48 ports.

- By default, port LED indicates data switching status of the port. LED Mode LED on the front panel of system LED block is solid green.
- If pressed the LED Mode button, the port LED indicates PoE power supply status of the port. LED Mode LED on the front panel of system LED block changes to solid amber.

S5860-48XMG

Front Panel Schematic

(1) Status LED	(2) MGMT LED	(3) PWR1 LED
(4) PWR2 LED	(5) FAN LED	(6) RJ45 10G port
(7) SFP28 25G port	(8) QSFP+ 40G port	-

Rear Panel Schematic

(1) RJ45 Management port	(2) Console port	(3) USB port
(4) PS1 (Power Supply)	(5) PS2	(6) FAN1
(7) FAN2	(8) FAN3	-

Switch System Characteristics

Mechanical dimension (W x D x H)	442 mm x 420 mm x 43.6 mm (17.40 in. x 16.54 in. x 1.72 in.)
RJ45 10G port	48
RJ45 10G port LED	48 x 1
RJ45 10/100/1G Management port	1
Console port	1
USB port	1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
QSFP+ 40G port	2
QSFP+ 40G port LED	2 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
FAN LED	1
MGMT LED	1
Power Supply	1+1
FAN	2+1
Working environment temperature	0°C to 45°C (32°F to 113°F)

S5860-24XMG

Front Panel Schematic

(1) Status LED	(2) MGMT LED	(3) PWR1 LED
(4) PWR2 LED	(5) FAN LED	(6) RJ45 Management port
(7) Console port	(8) RJ45 10G port	(9) SFP+ 10G port
(10) SFP28 25G port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	-	-

Switch System Characteristics

Mechanical dimension (W x D x H)	442 mm x 420 mm x 43.6 mm (17.40 in. x 16.54 in. x 1.72 in.)
RJ45 10G port	24
RJ45 10G port LED	24 x 1
RJ45 10/100/1G Management port	1
Console port	1
SFP+ 10G port	4
SFP+ 10G port LED	4 x 1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
FAN LED	1
MGMT LED	1
Power Supply	1+1
FAN	2+1
Working environment temperature	0°C to 45°C (32°F to 113°F)

S5860-48MG-U

Front Panel Schematic

(1) Status LED	(2) MGMT LED	(3) PWR1 LED
(4) PWR2 LED	(5) FAN LED	(6) LED Mode (LED)
(7) LED Mode (button)	(8) RJ45 5G port	(9) SFP28 25G port
(10) QSFP+ 40G port	-	-

Rear Panel Schematic

(1) RJ45 Management port	(2) Console port	(3) USB port
(4) PS1 (Power Supply)	(5) PS2	(6) FAN1
(7) FAN2	(8) FAN3	-

Switch System Characteristics

Mechanical dimension (W x D x H)	442 mm x 420 mm x 43.6 mm (17.40 in. x 16.54 in. x 1.72 in.)
RJ45 5G port	24
RJ45 5G port LED	24 x 1
RJ45 10/100/1G Management port	1
Console port	1
USB port	1
SFP28 25G port	4
SFP28 25G port LED	4 x 1
QSFP+ 40G port	2
QSFP+ 40G port LED	2 x 1
Status LED	1
PWR1 LED	1
PWR2 LED	1
FAN LED	1
MGMT LED	1
LED Mode (LED)	1
LED Mode (button)	1

Power Supply	1+1
FAN	2+1
Working environment temperature	0°C to 45°C (32°F to 113°F)

NOTE

UPoE and PoE button

The first 48 x5G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts.

LED Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 48 ports.

- By default, port LED indicates data switching status of the port. LED Mode LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. LED Mode LED on the front panel of system LED block changes to solid amber.

S5870-48T6S/S5870-48T6S-U

Front Panel Schematic

(1) System Status LED	(2) PSU1 LED	(3) FAN Status LED
(4) Location LED	(5) PSU2 LED	(6) PoE Status LED (Only for AS4625-54P)
(7) 48 x 1G RJ45 ports	(8) 6 x10G SFP+ ports	(9) USB port
(10) Console port	(11) Management Ethernet port	(12) Reset button

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical dimension	350.35mm (L: Depth) x 440mm (W: Width) x 44mm (H: Height)
Management port	1
RJ45 Console port	1
1G RJ45 port	48
10G SFP+ port	6
System Status LED	1
PSU1 LED	1
PSU2 LED	1
FAN Status LED	1
Location LED	1
PoE Status LED (Only for AS4625-54P)	1
USB port	1
Reset button	1
PSU	2
FRU (Fan Removable Unit)	3
Operating environment temperature	0ºC～45ºC

NOTE

PoE (Only for S5870-48T6S-U)

The 48 x 1G RJ45 ports on the front panel support PoE. Port1~Port40 support supports IEEE802.3at/af, the maximum output power supported is up to 30 watts, Port41~Port48 support IEEE802.3bt standard, the maximum output power supported is up to 90 watts.

S5870-48T6BC/S5870-48T6BC-U

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7)PRI LED	(8) PoE LED	(9) Reset button
(10) RJ45 port	(11) 25GbE SFP28	(12) 100GbE QSFP28
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
10M/100M/1G RJ45 port	48
25G SFP28	4
100G QSFP28	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1
PSU	2

FAN	3

***UPoE (S5870-48T6BC-U)**

The first 48 RJ45 ports on the front panel of S5870-48T6BC-U support UPoE, the maximum output power can be set to up to 90 watts, the default value is 30 watts.

N5850-48X6C

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP 28 port
(7) RJ45 port	(8) QSFP 28 port LED	(9) RJ45 port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

N8550-64C

Front Panel Schematic

(1) Location LED	(2) Diagnosis LED	(3) FAN Status LED
(4) PSU1 LED	(5) PSU1 LED	(6) QSFP28 ports
(7) RJ45 Console port	(8) Management Ethernet port	(9) USB port
(10)Reset button	-	-

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4

Switch System Characteristics

Mechanical dimension	2U high chassis: 580 mm (L: Depth) x 438.4mm (W: Width) x 88 mm (H: Height maximum)
Management port	1
RJ45 Console port	1
QSFP28 ports	64
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	3+1
Working environment temperature	0ºC～45ºC

N9550-32D

Front Panel Schematic

(1) Locator LED	(2) Diagnosis LED	(3) FAN Status LED
(4) PS1 LED	(5) PS2 LED	(6) SFP+ 10G management ports
(7) RJ45 10/100/1G Management port	(8) RJ45 Console port	(9) QSFP56-DD 400G ports
(10) Reset button	(11) USB port	(12) PTP Clock output

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	Height: 43.1mm (maximum), Width: 438.4mm,Depth: 536mm
SFP+ 10G management port	2
SFP+ 10G management port LED	1 x 2
RJ45 10/100/1G Management port	1
RJ45 Console port	1
QSFP56-DD 400G port	32
QSFP56-DD 400G port LED	4 x 32
Locator LED	1
Diagnosis LED	1
FAN Status LED	1
PS1 LED	1
PS2 LED	1
PS	1+1
FAN	5+1
Working environment temperature	0 to +45 Degree C

N5850-48S6C

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	-	-

S5870-48MX6BC-U

Front Panel Schematic

(1) System LED	(2) PSU1 LED	(3) STK1 LED
(4) FAN LED	(5) PSU2 LED	(6) STK2 LED
(7) PRI LED	(8) PoE LED	(9) Reset button
(10) RJ45 port	(11) 25GbE SFP28	(12) 100GbE QSFP28
(13) USB port	(14) Management Ethernet port	(15) Console port

Rear Panel Schematic

(1) PSU1	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	-

Switch System Characteristics

Mechanical Dimension	Within 1RU
Management-ethernet port	1
Console port	1
2.5G Base-T	36
10G Base-T	12
25G SFP28	4
100G QSFP28	2
PSU LED	2
STK LED	2
FAN LED	1
System LED	1
PRI LED	1
PoE LED	1
USB port	1
Reset button	1

PSU	2
FAN	3

***UPoE**

The first 48 RJ45 ports on the front panel of S5870-48MX6BC-U support UPoE, the maximum output power can be set to up to 90 watts, the default value is 30 watts.

S3410-24TS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) ID LED	(5) 10/100/1000BASE-T RJ45 port	(6) 1G/10G SFP+
(7) Console port	-	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.72"x17.32"x9.69" (43.6x440x246.1mm)
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	24
10/100/1000BASE-T RJ45 port LED	24
1G/10G SFP+ port	4
1G/10G SFP+ port LED	4
Status LED	1
PWR1 LED	1
PWR2 LED	1
ID LED	1
Power Supply	2 (1+1 Redundancy) Hot-swappable
FAN	1 Built-in
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

S3410L-24TF

Front Panel Schematic

(1) Status LED	(2) Console port	(3) 10/100/1000BASE-T RJ45 port
(4) 1G/10G SFP+	-	-

Rear Panel Schematic

(1) PSU (Power Supply)	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.75"x17.44"x10.24" (44.5x443x260mm)
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	24
10/100/1000BASE-T RJ45 port LED	24
1G SFP port	4
1G SFP port LED	4
Status LED	1
Power Supply	1 Built-in
FAN	Fanless
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

S3410L-24TF-P

Front Panel Schematic

(1) Status LED	(2) LED Mode LED	(3) LED Mode Button
(4) Console port	(5) 10/100/1000BASE-T RJ45 port	(6) SFP port

Rear Panel Schematic

(1) PSU (Power Supply)	(2) FAN	-

Switch System Characteristics

Mechanical dimension (HxWxD)	44mmx440mmx320mm
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	24
10/100/1000BASE-T RJ45 port LED	24
1G SFP port	4
1G SFP port LED	4
Status LED	1
LED Mode LED	1
*LED Mode button	1
Power Supply	1 Built-in
FAN	1 Built-in
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

***LED Mode button**

The 24x1G RJ45 ports on the front panel support PoE, the maximum output power supported is up to 30 watts.

LED Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 24 ports.

- By default, port LED indicates data switching status of the port. LED Mode LED on the front panel of system LED block is solid green.
- If pressed the LED Mode button, the port LED indicates PoE power supply status of the port. LED Mode LED on the front panel of system LED block changes to solid amber.

S3410-24TS-P

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) M1/M2 LED	(5) PoE LED	(6) PoE Button
(7) Console port	(8) USB port	(9) 10/100/1000BASE-T RJ45 port
(10) SFP port	(11) SFP+ 10G port	-

Rear Panel Schematic

(1) PS1 (Power Supply)	(2) PS2	-

Switch System Characteristics

Mechanical dimension (HxWxD)	44mmx440mmx320mm
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	24
10/100/1000BASE-T RJ45 port LED	24
100/1000M SFP port (Combo Port)	2
100/1000M SFP port (Combo Port) LED	2
SFP+ 10G port	2
SFP+ 10G LED	2
Status LED	1
PWR1 LED	1
PWR2 LED	1
M1/M2 LED	2
PoE LED	1
*PoE button	1
Power Supply	1+1
FAN	2 x Built-in Fans
Working environment temperature	32°F to 122°F (0ºC to 50ºC)

***PoE button**

The 24x1G RJ45 ports on the front panel support PoE, the maximum output power supported is up to 30 watts.

PoE button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 24 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

*__Combo Port__

- Ports ge-1/1/23 and ge-1/1/24 are combo ports that support 1G port speed. A combo port consists of a GE electrical interface and a GE optical interface separately on the front panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled.

The electrical port has a higher priority, that is, as long as the electrical port is plugged in, the electrical port takes effect, but the optical port is invalid.

- When configuring port speed, the combo ports (when worked as electrical ports) only support auto-negotiation mode, that is, configuring the force rate will not take effect for combo port when it works as an electrical port.

N8550-32C

Front Panel Schematic

(1) PSU1 LED	(2) PSU2 LED	(3) FAN Status LED
(4) Diagnosis LED	(5) Location LED	(6) 100G QSFP28 port
(7)10G SFP+ port	(8) RJ45 Console port	(9) Management Ethernet port
(10) USB port	(11)Reset button	-

Rear Panel Schematic

(1) PSU1(Power Supply Unit)	(2) PSU2	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5	(8) FAN6	-

Switch System Characteristics

Mechanical dimension	1U high and 515mm deep
Management port	1
RJ45 Console port	1
100G QSFP28 port	32
10G SFP+ port	2
Location LED	1
Diagnosis LED	1
FAN Status LED	1
PSU1 LED	1
PSU2 LED	1
USB port	1
PSU	1+1
FAN	6
Working environment temperature	0ºC～45ºC

S3410C-8TMS-P

Front Panel Schematic

(1) Status LED	(2) PoE LED	(3) Mode Button
(4) Console port	(5) 1G/10G SFP+ port	(6) 1G/2.5G/5G RJ45 port
(7) 10/100/1000BASE-T RJ45 port	-	-

Rear Panel Schematic

(1) PSU (Power Supply)	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	55mmx210mmx235mm
RJ45 Console port	1
1G/10G SFP+ port	2
1G/10G SFP+ port LED	2
10/100/1000BASE-T RJ45 port	8
10/100/1000BASE-T RJ45 port LED	8
1G/2.5G/5G RJ45 port	2
1G/2.5G/5G RJ45 port LED	2
Status LED	1
PoE LED	1
* Mode button	1
Power Supply	1 Built-in
Working environment temperature	32°F to 113°F (0ºC to 45ºC)

***PoE button**

The 2x5G and first 6x1G RJ45 ports on the front panel support PoE, the maximum output power supported is up to 30 watts.

Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the 8 PoE ports.

- By default, port LED indicates data switching status of the port. Mode LED on the front panel of system LED block is solid green.
- If pressed the Mode button, the port LED indicates PoE power supply status of the port. Mode LED on the front panel of system LED block changes to solid amber.

S3410C-16TF

Front Panel Schematic

(1) Status LED	(2) Console port	(3) 1G SFP port
(4) 10/100/1000BASE-T RJ45 port	-	-

Rear Panel Schematic

(1) PSU (Power Supply)	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	55mmx210mmx235mm
RJ45 Console port	1
1G SFP port	2
1G SFP port LED	2
10/100/1000BASE-T RJ45 port	16
10/100/1000BASE-T RJ45 port LED	16
Status LED	1
Power Supply	1 Built-in
Working environment temperature	32°F to 113°F (0ºC to 45ºC)

N5850-48S6Q

Front Panel Schematic

(1) PS1(Power Supply Status) LED	(2) PS2(Power Supply Status) LED	(3) Diag(Diagnostic) LED
(4) FAN LED	(5) LOC LED	(6) QSFP+ port
(7) SFP+ port	(8) QSFP+ port LED	(9) SFP+ port LED
(10) USB port	(11) Management Ethernet port	(12) Console port

Rear Panel Schematic

(1) PSU1 (removable power supply unit) one and two	(2) PSU2 (removable power supply unit)	(3) FAN1
(4) FAN2	(5) FAN3	(6) FAN4
(7) FAN5		

S3410C-16TMS-P

Front Panel Schematic

(1) Status LED	(2) PoE LED	(3) Mode Button
(4) Console port	(5) SFP+ 10G port	(6) 10M/100/1000MBASE-T ports
(7) 1000M/2.5G/5GBASE-T ports		

Rear Panel Schematic

(1) PSU (Power Supply Unit)	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	2.17"x8.27"x9.25"（55x210x235mm）
1/10G SFP+ port	2
1/10G SFP+ port LED	2
10M/100/1000MBASE-T ports	16
10M/100/1000MBASE-T ports LED	16
1000M/2.5G/5GBASE-T ports	2
1000M/2.5G/5GBASE-T ports LED	2
Status LED	1
Power Supply	1 Built-in
*Mode button	1
Console port	1
Working environment temperature	32°F to 113°F (0ºC to 45ºC)

***Mode button**

The 8x1G RJ45 ports on the front panel support PoE+, the maximum output power supported is up to 30 watts.

Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 8 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the Mode button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

S3410C-16TF-P

Front Panel Schematic

(1) Status LED	(2) PoE LED	(3) Mode Button
(4) Console port	(5) 1G SFP port	(6) 10M/100/1000MBASE-T ports

Rear Panel Schematic

(1) PS1 (Power Supply)	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	2.17"x8.27"x9.25"（55x210x235mm）
1G SFP port	2
1G SFP port LED	2
10M/100/1000MBASE-T ports	16
10M/100/1000MBASE-T ports LED	16
Status LED	1
Power Supply	1 Built-in
PoE LED	1
*Mode button	1
Console port	1
Working environment temperature	32°F to 113°F (0ºC to 45ºC)

***Mode button**

The 8x1G RJ45 ports on the front panel support PoE+, the maximum output power supported is up to 30 watts.

Mode button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 8 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the Mode button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

S3410-48TS-P

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) M1/M2 LED	(5) PoE LED	(6) PoE Button
(7) Console port	(8) USB port	(9) 10/100/1000BASE-T RJ45 port
(10) 1G SFP port (Combo)	(11) 10G SFP+ port	-

Rear Panel Schematic

(1) Expansion module slot1	(2) Expansion module slot2	(3) PS1 (Power Supply)
(4) PS2	(5) Grounding point	

Switch System Characteristics

Mechanical dimension (HxWxD)	44mmx440mmx360mm
RJ45 Console port	1
10/100/1000BASE-T RJ45 port	48
10/100/1000BASE-T RJ45 port LED	48
1G SFP port (Combo Port)	2
1G SFP port (Combo Port) LED	2
10G SFP+ port	2
10G SFP+ LED	2
Status LED	1
PWR1 LED	1
PWR2 LED	1
M1/M2 LED	2
PoE LED	1
*PoE button	1
Expansion module slot	2
Power supply	1+1
FAN	2 x Built-in Fans

Working environment temperature	32°F to 122°F (0ºC to 50ºC)

*__PoE button__

The 48x1G RJ45 ports on the front panel support PoE, the maximum output power supported is up to 30 watts.

PoE button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 48 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

*__Combo Port__

Ports ge-1/1/47 and ge-1/1/48 are combo ports that support 1G port speed. A combo port consists of a GE electrical interface and a GE optical interface separately on the front panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled.

- The electrical port has a higher priority, that is, as long as the electrical port is plugged in, the electrical port takes effect, but the optical port is invalid.
- When configuring port speed, the combo ports (when worked as electrical ports) only support auto-negotiation mode, that is, configuring the force rate will not take effect for combo port when it works as an electrical port.

S3410-48TS

Front Panel Schematic

(1) Status LED	(2) PWR1 LED	(3) PWR2 LED
(4) Console port	(5) RESET button	(6) ID LED
(7) 10M/100/1000MBASE-T ports	(8) SFP+ 10G port	-

Rear Panel Schematic

(1) PWR1 (Power Supply Unit)	(2) PWR2	(3) PWR1 LED
(4) PWR2 LED	(5) Fan	

Switch System Characteristics

Mechanical dimension (HxWxD)	1.75"x17.44"x10.55"(44.5×443×268mm)
10G SFP+ port	4
10G SFP+ port LED	4
10M/100/1000MBASE-T ports	48
10M/100/1000MBASE-T ports LED	48
Status LED	1
Power Supply	2 (1+1 Redundancy) Hot-swappable
Fan	1 Built-in
Console port	1
ID LED	1
Working environment temperature	0 to 50ºC (32 to122°F)

S3410L-48TF

Front Panel Schematic

(1) Status LED	(2) Console port	(3) SFP 1G port
(4) 10M/100/1000MBASE-T ports		

Rear Panel Schematic

(1) PSU (Power Supply Unit)	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.75"x17.44"x10.55"(44.5×443×268mm)
1G SFP port	4
1G SFP port LED	4
10M/100/1000MBASE-T ports	48
10M/100/1000MBASE-T ports LED	48
Status LED	1
Power Supply	1 Built-in
Fan	1 Built-in
Console port	1
Working environment temperature	0 to 50ºC (32 to122°F)

N8550-24CD8D

Front Panel Schematic

(1) SYS LED	(2) ID LED	(3) PSU LED
(4) FAN LED	(5) QSFP56 Port	(6) QSFP56 Port LED
(7) QSFP-DD Port	(8) QSFP-DD Port LED	-

Rear Panel Schematic

(1) PSU (1+1 Redundancy) Hot-swappable, AC	(2) PSU LED	(3) FAN (5+1 Redundancy)
(4) FAN LED	(5) MGMT Port	(6) MGMT LED
(7) Reset Button	(8) Console Port	(9) SYS LED
(10) USB Port	-	-

Switch System Characteristics

Mechanical dimension (HxWxD)	1.73"×17.32"× 25.98"(44× 440× 660mm)
QSFP56 port	24
QSFP56 port LED	48
QSFP-DD ports	8
QSFP-DD ports LED	8
SYS LED (Front Panel)	1
SYS LED (Rear Panel)	1
PSU	2 (1+1 Redundancy) Hot-swappable
PSU LED (Front Panel)	1
PSU LED (Rear Panel)	6
Fan	6 (5+1 Redundancy), Front-to-Back
Fan LED (Front Panel)	1
Fan LED (Rear Panel)	6
Console Port	1
ID LED	1
Reset Button	1

Console Port	1
USB Port	1
MGMT Port	1
MGMT Port LED	1
Working environment temperature	0°C to 40 °C (32°F to 104°F)

N9600-64OD

Front Panel Schematic

(1) Management Ethernet port	(2) LINK/ACT LED	(3) Console port
(4) USB port	(5) SYS LED	(6) BMC LED
(7) PSU LED	(8) FAN LED	(9) OSFP 800G ports
(10) SFP28 25G ports	-	-

Rear Panel Schematic

(1) FAN1	(2) FAN2	(3) FAN3
(4) FAN4	(5) PSU1	(6) PSU2

Switch System Characteristics

Mechanical dimension (H x W x D)	3.39"x 17.32"x 29.92" (86.1 x 440 x 760mm)
800G OSFP ports	64
800G OSFP port LED	64
25G SFP28 ports	2
25G SFP28 ports LED	2
BMC LED	1
PSU LED (front panel)	1
FAN LED (front panel)	1
SYS LED	1
LINK/ACT LED	1
Power supply	2 (1+1 Redundancy) Hot-swappable, AC
Fan	4 (3+1 Redundancy) Hot-swappable, Front-to-Back
PSU LED (rear panel)	2
FAN LED (rear panel)	4
Working environment temperature	0 to 40ºC (32 to104°F)

Indicator Light on Switch Panel

Due to the differences between the platforms, this feature is categorized by platform.
The port of RJ45 LED's schematic diagram:

_____

L		R

---- ----



L is the left port; R is the right port.

> **Note**
> For the Trident II switch, if user attaches the copper RJ45 module, the port LED will light up, even without a cable plugged in.

- Dell Switches
  - Z9100-ON Switch
  - S4128F-ON/S4128T-ON Switch
  - N3208PX-ON Switch
  - N3224P-ON/N3224F-ON/N3224T-ON Switch
  - N3224PX-ON Switch
  - N3248P-ON/N3248TE-ON Switch
  - N3248PXE-ON/N3248X-ON Switch
  - N3248TE-ON Switch
  - S4048 Switch
  - S4148T-ON/S4148F-ON Switch
  - S5212F-ON Switch
  - S5224F-ON Switch
  - S5248F Switch
  - S5296F-ON Switch
  - Z9264F-ON Switch
  - S5232F-ON Switch
  - N2224X-ON/N2224PX-ON Switch
  - N2248X-ON/N2248PX-ON Switch
- EdgeCore/Accton Switches
  - AS4610 Serial Switch
  - AS4625-54P/AS4625-54T Switch
  - AS4630-54NPE Switch
  - AS7816-64X Switch
  - AS5835-54X Switch
  - AS4630-54PE Switch
  - AS5712-54X Switch
  - AS9716-32D Switch
  - AS7312-54X/AS7312_54XS Switch
  - AS5812-54T Switch
  - AS5812-54X Switch
  - AS5835-54T Switch
  - AS6712-32X Switch
  - AS6812_32X Switch
  - AS7326-56X Switch
  - AS7712-32X Switch
  - AS7726-32X Switch
- Delta/Agema Switches
  - AG9032v1 Switch
  - AG5648V1 Switch
  - AG7648 Switch
- FS Switches
  - N5850-48S6C Switch
  - N8550-32C Switch
  - N5850-48S6Q Switch
  - S5810-48TS-P Switch
  - S5810-28FS Switch
  - S5810-28TS Switch
  - S5810-48FS Switch
  - S5810-48TS Switch

- S5860-20SQ Switch
- S5860-24XB-U Switch
- N8560-32C Switch
- N8560-64C Switch
- S5860-24MG-U Switch
- S5860-48XMG-U Switch
- S5860-24XMG Switch
- S5860-48MG-U Switch
- S5860-48XMG Switch
- S5870-48T6S/S5870-48T6S-U Switch
- S5870-48T6BC/S5870-48T6BC-U Switch
- N5850-48X6C Switch
- N8550-64C Switch
- N9550-32D Switch
- S5870-48MX6BC-U Switch
- S3410-24TS Switch
- S3410L-24TF Switch
- S3410L-24TF-P Switch
- S3410-24TS-P Switch
- S3410C-8TMS-P Switch
- S3410C-16TF Switch
- S3410C-16TMS-P Switch
- S3410C-16TF-P Switch
- S3410-48TS-P Switch
- N8550-48B8C Switch
- S3410-48TS Switch
- S3410L-48TF Switch
- N8550-24CD8D Switch
- N9600-64OD Switch

Dell Switches

- Z9100-ON Switch
- S4128F-ON/S4128T-ON Switch
- N3208PX-ON Switch
- N3224P-ON/N3224F-ON/N3224T-ON Switch
- N3224PX-ON Switch
- N3248P-ON/N3248TE-ON Switch
- N3248PXE-ON/N3248X-ON Switch
- N3248TE-ON Switch
- S4048 Switch
- S4148T-ON/S4148F-ON Switch
- S5212F-ON Switch
- S5224F-ON Switch
- S5248F Switch
- S5296F-ON Switch
- Z9264F-ON Switch
- S5232F-ON Switch
- N2224X-ON/N2224PX-ON Switch
- N2248X-ON/N2248PX-ON Switch

Z9100-ON Switch

·System LED Definition：

LED	Status	Description
System Status LED	Solid Green	all functions are normal
	Flashing Green with 2 sec on and 1 sec off	Booting
	Solid Amber	Major Fault
	Flashing Amber with 2 sec on and 1 sec off	Minor Fault
Power Status LED	Solid Green	Normal
	Solid Amber	POST in progress
	Flashing Amber with 2 sec on and 1 sec off	Power supply fault
	Off	Off
Fan Status LED	Solid Green	all functions are normal
	Flashing Amber with 2sec on and 1 sec off	One of Fan or Fan tray fault
	Other	Off
System Beacon LED	Off	Idle
	Flashing Blue with 1sec on and 1 sec off	beacon
Platform Stacking LED	Not supported.	

·QSFP28 port status LED Definition：

LED	Status	Description
1st LED	Solid Green	Port linked operating at max port speed, i.e. running 100G on QSFP28 port
	Flash Green (~30ms)	Port Activity operating at max port speed, i.e. running 100G on QSFP28 port
	Solid Amber	Port linked operating at lower speed, i.e. running 40G or 10G on QSFP28 port.
	Flashing Amber (~30ms)	Port Activity operating at lower speed, i.e. running 40G or 10G on QSFP28 port.
	Off	No link
	Flashing Amber with 1 sec on and 1 sec off	Port Beacon
All four LEDs are used when 4x25G mode or 4x10G mode is running on QSFP28 port.	Solid Green	4x25G Link on QSFP28 port
	Solid Amber	4x10G Link on QSFP28 port
	Flashing (~30ms) Green	4x25G Activity on QSFP28 port
	Flashing (~30ms) Amber	4x10G Activity on QSFP28 port
	Off	No link
	Flashing Amber with 1 sec on and 1 sec off	Port Beacon
1st and 3rd LEDs are used when 2x40G mode is running on QSFP28 port.	Solid Amber	2x40G Link on QSFP28 port
	Flashing (~30ms) Amber	2x40G Activity on QSFP28 port
	Off	No link
	Flashing Amber with 1 sec on and 1 sec off	Port Beacon

·SFP+ port status LED Definition：

LED	Status	Description
One Port Link/ Activity Status Green/Amber bi-color LEDs is	Solid Green	Port linked operating at max port speed, i.e. running 10G on SFP+ port
	Flash Green (~30ms)	Port Activity operating at max port speed, i.e. running 10G on SFP+ port
	Solid Amber	Port linked operating at lower speed, i.e. running 1G on SFP+ port.

LED	Status	Description
provided for each front panel port	Flashing Amber (~30ms)	Port Activity operating at lower speed, i.e. running 1G on SFP+ port.
	Off	No link
	Flashing Amber with 1 sec on and 1 sec off	Port Beacon

S4128F-ON/S4128T-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid Green – all functions are normal. • Flashing Green – Booting. Flashing Green with 2 sec on and 1 sec off • Solid Amber – Major Fault. Displays summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber – Major Fault. Flashing Amber with 2 sec on and 1 sec off Displays summary of all major faults within the system; the faults are not traffic affecting.	At front
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Flashing Amber with 2sec on and 1 sec off. Power supply fault. • Off – No power.	At front
FAN LED	• Solid Green – all functions are normal. • Flashing Amber – One of the Fans or Fan tray fault. Flashing Amber with 2 sec on and 1 sec off.	At front
Beacon LED	Not in use.	At front
Stacking LED	Not in use.	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

10GBT port LEDs

Feature	Detailed Description
10GBT LED	• Off – No Link • Solid Green – Link on 10G speed • Flashing Green(~30ms) – Port Activity operating at 10G speed. • Solid Amber – Port Link operating at lower speed. • Flashing Amber (~30ms)–Port Activity operating at lower speed. • Solid Blue –Port Beacon/Locater

SFP+ port LEDs

Feature	Detailed Description

SFP+ port LED	• Link LED: Green/Amber
	  ◦ Solid Green = Port linked operating at max port speed, i.e. running 10G on SFP+ port
	  ◦ Solid Amber = Port linked operating at lower speed, i.e. running 1G on SFP+ port.
	  ◦ Flashing Amber with 1 sec on and 1 sec off -Port Beacon
	  ◦ Off = No link
	• Activity LED: Green
	  ◦ Off – There is no current transmit/ receive activity.
	  ◦ Flashing Green(~30ms) Port Activity.

QSFP28 port LEDs

1) 1st LED

Feature	Detailed Description
Link/ACT LED	• Solid Green = Port link operating at max port speed, i.e. running 100G on QSFP28 port • Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G on QSFP28 port • Solid Amber = Port link operating at lower speed, i.e. running 40G on QSFP28 port. • Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40G on QSFP28 port. • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

2) All four LEDs shall be used when 4x25G or 10G mode is running on QSFP28 port

Feature	Detailed Description
Link/ACT LED	• Solid Green = 4x25G Link on QSFP28 port • Solid Amber = 4x10G Link on QSFP28 port • Flashing (~30ms) Green = 4x25G Activity on QSFP28 port • Flashing (~30ms) Amber = 4x10G Activity on QSFP28 port • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

3) 1st and 3rd LEDs shall be used when 2x50G mode is running on QSFP28 port

Feature	Detailed Description
Link/ACT LED	• Solid Amber = 2x50G Link on QSFP28 port • Flashing (~30ms) Amber = 2x50G Activity on QSFP28 port • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

Management Ethernet port LEDs

Feature	Detailed Description
Link LED	• Off – No Link • Solid Green – Port link operating at 1G speed. • Solid Amber – Port link operating at 10/100M speed.
Activity	• Off – No Activity • Flashing Green – Port Activity.

N3208PX-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green with 2 sec on and 1 sec off – Booting • Solid Amber – Major Fault • Flashing Amber with 2 sec on and 1 sec off – Minor Fault	At front
Power Status LED (Bi-color LED)	• Solid Green – Normal • Solid Amber – POST in progress • Flashing Amber with 2 sec on and 1 sec off – PSU fault • Off – No power	At front
FAN Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Amber with 2 sec on and 1 sec off – Fan tray fault	At front
System Beacon LED	• Off – Idle • Flashing Blue with 1 sec on and 1 sec off – (SID in Dell parlance)	At front

Port LED Definition

1000Base-T Copper Ethernet Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Solid Green – Link at 1000Base-T (Max) • Solid Amber – Link at 10/100MBase-T • OFF – No Link
ACT/POE LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off – No Activity, PoE Power Off

2.5G/5GBase-T Copper Ethernet Port LEDs

Feature	Detailed Description

LINK/SPD LED (Left bi-color LED)	• Solid Green – Link at 5GBase-T (Max) • Solid Amber – Link at 10/100/1000MBase-T or 2.5GBase-T • Off – No Link
ACT/POE LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

10GbE SFP+ Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green –Link at 10GE Speed • Solid Amber –Link at lower than 10GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking Green (~30ms) – Activity

OOB Ethernet Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link on 1000Base-T • Solid Amber – Link on 10/100MBase-T
ACT LED **(**Right single color LED**)**	• Off – No Link • Blinking Green (~30ms) – Activity

Console port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green-all functions are normal. • Flashing Green – Booting • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

2.5G/5G/10GBase-T Copper Ethernet Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Solid Green – Link at 10GBase-T (Max) • Solid Amber – Link at 10/100/1000MBase-T or 2.5/5/10GBase-T • Off – No Link
ACT/POE LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

25GbE SFP28 Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green –Link at 25GE Speed • Solid Amber –Link at lower than 25GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking Green (~30ms) – Activity

Stacking (QSFP28) Port LEDs

Feature	Detailed Description
LINK/ACT LED (Bi-color LED)	**1st LED: Green/Amber** • Solid Green = Port linked operating at max port speed, i.e. running 100GbE o QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)

	• Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Off = No link Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance a 1.5ft = 180+10 cd/m2) All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running o QSFP28 port. • Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45+5cd/m2) • Off = No link Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance a 1.5ft = 180+10 cd/m2)

OOB Ethernet Port LEDs

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green – Link at 1000Base-T • Solid Amber – Link at 10/100MBase-T

ACT LED (Right single color LED)	• Off – No Link • Blinking Green (~30ms) – Activity

Console Port LEDs

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green – Link

N3224PX-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all functions are normal. • Flashing Green – Booting. • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

2.5G/5G/10GBase-T Copper Ethernet Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Solid Green – Link at 10GBase-T (Max) • Solid Amber – Link at 10/100/1000MBase-T or 2.5/5/10GBase-T • Off – No Link
ACT/POE LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

25GbE SFP28 Port LEDs

Feature	Detailed Description
LINK/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green –Link at 25GE Speed • Solid Amber –Link at lower than 25GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking Green (~30ms) – Activity

Stacking (QSFP28) Port LEDs

Feature	Detailed Description

LINK/ACT LED
(Bi-color LED)
	• 1st LED: Green/Amber
	  ◦ Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Off = No link
	  ◦ Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)
	• All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port.
	  ◦ Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
	  ◦ Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45+5cd/m2)
	  ◦ Off = No link
	  ◦ Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

OOB Ethernet Port LEDs

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green – Link at 1000Base-T • Solid Amber – Link at 10/100MBase-T
ACT LED (Right single color LED)	• Off – No Link • Blinking Green (~30ms) – Activity

Console Port LEDs

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green – Link

N3248P-ON/N3248TE-ON Switch

System LED Definition

Feature	Detailed Description	Comment
Platform Stacking LED	Not supported.	At front
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green with 2 sec on and 1 sec off – Booting • Solid Amber – Major Fault • Flashing Amber with 2 sec on and 1 sec off – Minor Fault	At front
Power Status LED (Bi-color LED)	• Solid Green – Normal • Solid Amber – POST in progress • Flashing Amber with 2 sec on and 1 sec off – PSU fault • Off – No power	At front
FAN Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Amber with 2 sec on and 1 sec off – Fan tray fault	At front
System Beacon LED	• Off – Idle • Flashing Blue with 1 sec on and 1 sec off – (SID in Dell parlance)	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

1000Base-T copper port LEDs

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Solid Green – Link at 1000Base-T (Max) • Solid Amber – Link at 10/100MBase-T • Off – No Link
POE/ACT LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

10GbE SFP+ Port LEDs:

Feature	Detailed Description
Link/SPD LED	• Off – No Link

(Left bi-color LED)	• Solid Green –Link at 10GE Speed • Solid Amber –Link at lower than 10GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking green (~30ms) – Activity

Stacking (QSFP28) Port LEDs:

Feature	Detailed Description
LINK/ACT LED (Bi-color LED)	• 1st LED: Green/Amber ◦ Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) ◦ Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) ◦ Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) ◦ Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) ◦ Off = No link ◦ Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2) • All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port. ◦ Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) ◦ Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) ◦ Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. ◦ Green (Luminance at 1.5ft = 45+5 cd/m2) ◦ Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. ◦ Amber (Luminance at 1.5ft = 45+5cd/m2) ◦ Off = No link ◦ Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

OOB Ethernet Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link on 1000Base-T • Solid Amber – Link on 10/100MBase-T
ACT LED (Right single color LED)	• Off – No Link • Blinking Green (~30ms) – Activity

Console port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link

N3248PXE-ON/N3248X-ON Switch

System LED Definition

Feature	Detailed Description	Comment
Platform Stacking LED	Not supported.	At front
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green with 2 sec on and 1 sec off – Booting • Solid Amber – Major Fault • Flashing Amber with 2 sec on and 1 sec off – Minor Fault	At front
Power Status LED (Bi-color LED)	• Solid Green – Normal • Solid Amber – POST in progress • Flashing Amber with 2 sec on and 1 sec off – PSU fault • Off – No power	At front
FAN Status LED (Bi-color LED)	• Solid Green – all functions are normal • Solid Amber – Fan tray fault	At front
System Beacon LED	• Off – Idle • Flashing Blue with 1 sec on and 1 sec off – (SID in Dell parlance)	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

1G/2.5G/5G/10G copper port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Solid Green – Link at 10GBase-T (Max) • Solid Amber – Link at 10/100/1000MBase-T or 2.5/5GBase-T • Off – No Link
POE/ACT LED (Right bi-color LED) (On N3248PXE-ON)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

25GbE SFP28 Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green –Link at 25GE Speed • Solid Amber –Link at lower than 25GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking green (~30ms) – Activity

Stacking (QSFP28) Port LEDs:

Feature	Detailed Description
LINK/ACT LED (Bi-color LED)	**1st LED: Green/Amber** • Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2) **All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port.** • Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. • Green (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. • Amber (Luminance at 1.5ft = 45+5cd/m2) • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

OOB Ethernet Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link on 1000Base-T • Solid Amber – Link on 10/100MBase-T

ACT LED **(**Right single color LED**)**	• Off – No Link • Blinking Green (~30ms) – Activity

Console port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link

N3248TE-ON Switch

System LED Definition

Feature	Detailed Description	Comment
Platform Stacking LED	Not supported.	At front
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green with 2 sec on and 1 sec off – Booting • Solid Amber – Major Fault • Flashing Amber with 2 sec on and 1 sec off – Minor Fault	At front
Power Status LED (Bi-color LED)	• Solid Green – Normal • Solid Amber – POST in progress • Flashing Amber with 2 sec on and 1 sec off – PSU fault • Off – No power	At front
FAN Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Amber with 2 sec on and 1 sec off – Fan tray fault	At front
System Beacon LED	• Off – Idle • Flashing Blue with 1 sec on and 1 sec off – (SID in Dell parlance)	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

1000Base-T copper port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Solid Green – Link at 1000Base-T (Max) • Solid Amber – Link at 10/100MBase-T • Off – No Link
POE/ACT LED (Right bi-color LED)	• Blinking Green (~30ms) – Activity, PoE Power Off (Activity for Non-P) • Blinking Amber (~30ms) – Activity, PoE Power On • Solid Amber – No Activity, PoE Power On • Off –No Activity, PoE Power Off

10GbE SFP+ Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid Green –Link at 10GE Speed • Solid Amber –Link at lower than 10GE Speed
ACT LED (Right bi-color LED)	• Off – No Activity • Blinking green (~30ms) – Activity

Stacking (QSFP28) Port LEDs:

Feature	Detailed Description
LINK/ACT LED (Bi-color LED)	1st LED: Green/Amber • Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 25GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2) All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port. • Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2) • Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. • Green (Luminance at 1.5ft = 45+5 cd/m2) • Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. • Amber (Luminance at 1.5ft = 45+5cd/m2) • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

OOB Ethernet Port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link on 1000Base-T • Solid Amber – Link on 10/100MBase-T

ACT LED (Right single color LED)	• Off – No Link • Blinking Green (~30ms) – Activity

Console port LEDs:

Feature	Detailed Description
Link/SPD LED (Left bi-color LED)	• Off – No Link • Solid green – Link

S4048 Switch

System LED Definition

Feature	Detailed Description	Comment
Power LED	• Off = No power • Solid Amber = POST in process • Blinking Amber = Power Supply failed • Solid Green = Normal	At front side
FAN LED	• Solid green = fan powered and @expected rpm • Solid yellow = fan failed including incompatible airflow direction from what is indicated in the Board ID for the particular SKU.	At front side
PSU LED	• Solid green = The DC output is on and OK . • Solid yellow = Power supply critical event causing a shutdown; failure,OCP, OVP, Fan Fail, OTP,UVP . • Blinking yellow =Power supply warning events where the power supply continues to operate; high temp (PMBus reading inlet > 60deg; PMBus reading hotspot >100deg), high power, high current (105 %*), slow fan.	At the rear side
MASTER LED	Not supported.	At front side
LOCATED LED	Not supported.	At front side
7-DIGIT Stack LED	Not supported.	At front side
Health LED	Not supported.	At front side

⚠

For FAN LED , when one of FAN LEDs on the rear side failed , fan led on the front panel will display yellow.

SFP+ port LED Definition

Feature	Detailed Description	Comment
Link LED	• Off – No Link • Solid green – Link on 10G speed • Solid amber – Link on 1G speed	-
Activity LED	• Off – No Link • Blinking green – Transmit/Receive is activity	-

QSFP+ port LED Definition

Feature	Detailed Description	Comment
Link/ACT LED	• Off – No Link • Solid green – Link on 40G speed • Solid Amber- Link on 10G speed • Blinking green – 40G speed ,transmit/Receive is activity • Blinking amber – 10G speed ,transmit/Receive is activity	-

Front Management Ethernet port LED Definition

Feature	Detailed Description	Comment
Link LED	• Off – No Link • Solid green – Link on 1G speed • Solid yellow – Link on 10M/100M speed	-
Activity	• Off – No Link • Blinking green – Transmit/Receive is activity	-

S4148T-ON/S4148F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all function are normal. • Flashing Green – Booting. Flashing Green with 2 sec on and 1 sec off • Solid Amber – Major Fault. Displays summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber – Major Fault. Flashing Amber with 2 sec on and 1 sec off Displays summary of all major faults within the system; the faults are not traffic affecting.	At front
Power LED	• Solid Green – Normal. • Solid Amber – Post in progress. • Flashing Amber – Flashing Amber with 2sec on and 1 sec off. Power supply fault. • Off – No power.	At front
FAN LED	• Solid Green – all function are normal. • Flashing Amber – One of Fan or Fan tray fault. Flashing Amber with 2 sec on and 1 sec off.	At front
Beacon LED	Not in use.	At front
Stacking LED	Not in use.	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

10GBT port LEDs

Feature	Detailed Description
10GBT LED	• Off – No Link • Solid Green – Link on 10G speed • Flashing Green(~30ms) – Port Activity operating at 10G speed. • Solid Amber – Port Linked operating at lower speed. • Flashing Amber (~30ms)–Port Activity operating at lower speed. • Solid Blue –Port Beacon/Locater

SFP+ port LEDs

Feature	Detailed Description
SFP+ port LED	• Link LED: Green/Amber

	◦ Solid Green = Port linked operating at max port speed, i.e. running 10G on SFP+ port ◦ Solid Amber = Port linked operating at lower speed, i.e. running 1G on SFP+ port. ◦ Flashing Amber with 1 sec on and 1 sec off -Port Beacon ◦ Off = No link • Activity LED: Green ◦ Off – There is no current transmit/ receive activity. ◦ Flashing Green(~30ms) Port Activity.

QSFP28 port LEDs

1) 1st LED:

Feature	Detailed Description
Link/ACT LED	• Solid Green = Port linked operating at max port speed, i.e. running 100G on QSFP28 port • Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G on QSFP28 port • Solid Amber = Port linked operating at lower speed, i.e. running 40G on QSFP28 port. • Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40G on QSFP28 port. • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

2) All four LEDs shall be used when 4x25G or 10G mode is running on QSFP28 port.

Feature	Detailed Description
Link/ACT LED	• Solid Green = 4x25G Link on QSFP28 port • Solid Amber = 4x10G Link on QSFP28 port • Flashing (~30ms) Green = 4x25G Activity on QSFP28 port • Flashing (~30ms) Amber = 4x10G Activity on QSFP28 port • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

3) 1st and 3rd LEDs shall be used when 2x50G mode is running on QSFP28 port.

Feature	Detailed Description
Link/ACT LED	• Solid Amber = 2x50G Link on QSFP28 port • Flashing (~30ms) Amber = 2x50G Activity on QSFP28 port • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

QSFP+ port LEDs

1) 1st LED:

Feature	Detailed Description
Link/ACT LED	• Solid Green = Port linked operating at 40G. • Flashing Green (~30ms) =Port Activity operating at 40G • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

2) All four LEDs shall be used when 4x10G or 1G mode is running on QSFP+ port.

Feature	Detailed Description
Link/ACT LED	• Solid Green = 4x10G Link on QSFP+ port • Solid Amber = 4x1G Link on QSFP+ port • Flashing (~30ms) Green = 4x10G Activity on QSFP+ port • Flashing (~30ms) Amber = 4x1G Activity on QSFP+ port • Off = No link • Flashing Amber with 1 sec on and 1 sec off – Port Beacon

Management Ethernet port LEDs

Feature	Detailed Description
Link LED	• Off – No Link • Solid Green – Port linked operating at 1G speed. • Solid Amber – Port linked operating at 10/100M speed.
Activity	• Off – No Activity • Flashing Green – Port Activity.

S5212F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
Platform Stacking LED	Not in use.	At front
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green with 2 sec on and 1 sec off – Booting • Solid Amber – Major Fault • Flashing Amber with 2 sec on and 1 sec off – Minor Fault	At front
Power Status LED (Bi-color LED)	• Solid Green – Normal. • Solid Amber – POST in progress • Flashing Amber with 2 sec on and 1 sec off – PSU fault • Off – No power	At front
FAN Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Amber with 2 sec on and 1 sec off – Fan tray fault	At front
System Beacon LED	Not in use.	At front
7-DIGIT Stack LED	Not in use.	At front

Port LED Definition

SFP28 port status LED Indications:

One Port Link/ Activity Status Green/Amber bi-color LEDs is provided for each front panel port
Solid Green = Port linked operating at max port speed, i.e. running 25G on SFP28 port
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 25G on SFP28 port
Solid Amber = Port linked operating at lower speed, i.e. running 10/1G on SFP28 port.
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 10/1G on SFP28 port.
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

QSFP28 port status LED Indications:

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 100G on QSFP28 port

Flashing Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G on QSFP28 port
Solid Amber = Port linked operating at lower speed, i.e. running 40G or 10G on QSFP28 port.
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40G or 10G on QSFP28 port.
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon
All four LEDs are used when 4x25G mode or 4x10G mode is running on QSFP28 port.
Solid Green = 4x25G Link on QSFP28 port
Solid Amber = 4x10G Link on QSFP28 port
Flashing (~30ms) Green = 4x25G Activity on QSFP28 port
Flashing (~30ms) Amber = 4x10G Activity on QSFP28 port
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

S5224F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all functions are normal or PICOS is booting. • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

QSFP28 port status LED Indications

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 40GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)
All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port.
Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link

Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

SFP28 port status LED Indications

One Port Link/ Activity Status Green/Amber bi-color LED shall be provided for each front panel port.
Solid Green = Port linked operating at max port speed, i.e. running 25G Ethernet on SFP28 port Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 25G Ethernet on SFP28 port Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 10/1G Ethernet on SFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 10/1G Ethernet on SFP28 port. Amber (Luminance at 1.5ft = 180+10 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

S5248F Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all function are normal. • Flashing Green – Booting. Flashing Green with 2 sec on and 1 sec off. • Solid Amber –Major Fault. Displays summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Displays summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all function are normal. • Flashing Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

QSFP-DD port

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 200GbE on QSFP-DD port. Green (Luminance at 1.5ft = 45±5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 200GbE on QSFP-DD port. Green (Luminance at 1.5ft = 45±5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 100GbE or 40GbE or 10GbE on QSFP-DD port. Amber (Luminance at 1.5ft = 45±5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 100GbE or 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45±5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon Amber (Luminance at 1.5ft = 180±10 cd/m2)

All eight LEDs shall be used when 8x25GbE mode or 8x10GbE mode is running on QSFP-DD port.
Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45±5 cd/m2)
Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45±5 cd/m2)
Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45±5 cd/m2)
Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45±5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180±10 cd/m2)
1st and 5th LEDs shall be used when 2x100GbE mode is running on QSFP-DD port.
Solid Green = 2x100GbE Link on QSFP28 port. . Green (Luminance at 1.5ft = 45±5 cd/m2)
Flashing (~30ms) Green = 2x100GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45±5 cd/m2) Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180±10 cd/m2)
1st & 2nd and 5th & 6th LEDs shall be used when 4x50GbE mode is running on QSFP-DD port. (1st & 2nd LEDs for 1st 2x50GbE port and 5th & 6th LEDs for 2nd 2x50GbE port)
Solid Green = 2x50GbE Link on QSFP-DD port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Green = 2x50GbE Activity on QSFP-DD port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

QSFP28 port status LED

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100GbE on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon Amber (Luminance at 1.5ft = 180+10 cd/m2)
All four LEDs shall be used when 4x25GbE mode or 4x10GbE mode is running on QSFP28 port.
Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)

Solid Amber = 4x10GbE Link on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)
1st and 3rd LEDs shall be used when 2x50GbE mode is running on QSFP28 port.
Solid Green = 2x50GbE Link on QSFP28 port. Green(Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Green = 2x50GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon.Amber (Luminance at 1.5ft = 180+10 cd/m2)

SFP28 port status LED

One Port Link/ Activity Status Green/Amber bi-color LED shall be provided for each front panel port.
Solid Green = Port linked operating at max port speed, i.e. running 25G Ethernet on SFP28 port Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 25G Ethernet on SFP28 port Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 10/1G Ethernet on SFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 10/1G Ethernet on SFP28 port. Amber (Luminance at 1.5ft = 180+10 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

S5296F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	Solid green – all functions are normal or PICOS is booting. Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	Solid Green – Normal or POST in progress.. Flashing Amber – Power supply fault. Off – No power.	At front side
FAN LED	Solid Green – all functions are normal. Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

QSFP28 port status LED Indications

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 100G on QSFP28 port
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G on QSFP28 port
Solid Amber = Port linked operating at lower speed, i.e. running 40G on QSFP28 port.
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40G or 10G on QSFP28 port.
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon
All four LEDs are used when 4x25G mode or 4x10G mode is running on QSFP28 port.
Solid Green = 4x25G Link on QSFP28 port
Solid Amber = 4x10G Link on QSFP28 port
Flashing (~30ms) Green = 4x25G Activity on QSFP28 port
Flashing (~30ms) Amber = 4x10G Activity on QSFP28 port

Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

SFP28 port status LED Indications

One Port Link/ Activity Status Green/Amber bi-color LEDs is provided for each front panel port
Solid Green = Port linked operating at max port speed, i.e. running 25G on SFP28 port
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 25G on SFP28 port
Solid Amber = Port linked operating at lower speed, i.e. running 10/1G on SFP28 port.
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 10/1G on SFP28 port.
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

Z9264F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all function are normal. • Flashing Green – Booting. Flashing Green with 2 sec on and 1 sec off. • Solid Amber – Major Fault. Displays summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber – Major Fault. Flashing Amber with 2 sec on and 1 sec off Displays summary of all major faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – Post in progress. • Flashing Amber – Flashing Amber with 2sec on and 1 sec off. Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all function are normal. • Flashing Amber – One of Fan or Fan tray fault. • Flashing Amber with 2 sec on and 1 sec off. **Note:** The fan led on the front panel will display Amber if one of FAN LEDs on the rear side failed.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

QSFP28 port LEDs

1) 1st LED:

Feature	Detailed Description
Link/ACT LED	Four Port Link/ Activity Status Green/Amber bi-color LEDs shall be provided for each front QSFP28 port. 1 st LED: Green/Amber • Solid Green = Port linked operating at max port speed, i.e. running 100G on QSFP28 port. • Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G on QSFP28 port. • Solid Amber = Port linked operating at lower speed, i.e. running 40G or 10G on QSFP28 port.

	• Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40G or 10G on QSFP28 port. • Off = No link. • Flashing Amber with 1 sec on and 1 sec off – Port Beacon.

2) All four LEDs shall be used when 4x25G or 10G mode is running on QSFP28 port.

Feature	Detailed Description
Link/ACT LED	All four LEDs shall be used when 4x25G mode or 4x10G mode is running on QSFP28 port. • Solid Green = 4x25G Link on QSFP28 port. • Solid Amber = 4x10G Link on QSFP28 port. • Flashing (~30ms) Green = 4x25G Activity on QSFP28 port. • Flashing (~30ms) Amber = 4x10G Activity on QSFP28 port. • Off = No link. • Flashing Amber with 1 sec on and 1 sec off – Port Beacon.

3) 1st and 3rd LEDs shall be used when 2x50G mode is running on QSFP28 port.

Feature	Detailed Description
Link/ACT LED	1 st and 3 rd LEDs shall be used when 2x50G mode is running on QSFP28 port. • Solid Amber = 2x50G Link on QSFP28 port. • Flashing (~30ms) Amber = 2x50G Activity on QSFP28 port. • Off = No link. • Flashing Amber with 1 sec on and 1 sec off – Port Beaco.

SFP+ port LEDs

Feature	Detailed Description
SFP+ port LED	Link LED: Green/Amber • Solid Green = Port linked operating at max port speed, i.e.running 10G on SFP+ port • Solid Amber = Port linked operating at lower speed, i.e. running 1G on SFP+ port. • Flashing Amber with 1 sec on and 1 sec off – Port Beacon • Off = No link Activity LED: Green • Off – There is no current transmit/ receive activity. • Flash Green (~30ms) – Port Activity

S5232F-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all functions are normal or PICOS is booting. • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

SFP+ port status LED Indications

One Port Link/ Activity Status Green/Amber bi-color LED shall be provided for each front panel port.
Solid Green = Port linked operating at max port speed, i.e. running 10GbE on SFP+ port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 10GbE on SFP+ port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 1GbE on SFP+ port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 1GbE on SFP+ port. Amber (Luminance at 1.5ft = 180+10 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon

QSFP28 port status LED Indications

1st LED: Green/Amber

Solid Green = Port linked operating at max port speed, i.e. running 100G Ethernet on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flash Green (~30ms) = Port Activity operating at max port speed, i.e. running 100G Ethernet on QSFP28 port Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. running 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity operating at lower speed, i.e. running 40GbE or 10GbE on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)
All four LEDs are used when 4x25G mode or 4x10G mode is running on QSFP28 port.
Solid Green = 4x25GbE Link on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = 4x10GbE Link on QSFP28 port.Amber (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Green = 4x25GbE Activity on QSFP28 port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing (~30ms) Amber = 4x10GbE Activity on QSFP28 port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No link
Flashing Amber with 1 sec on and 1 sec off – Port Beacon. Amber (Luminance at 1.5ft = 180+10 cd/m2)

N2224X-ON/N2224PX-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	Solid green – all functions are normal. • Flashing Green – Booting. • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Power supply fault. Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

N2224PX RJ45 port status LED Indications

Left Link/Speed LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. if auto-negotiated/forced to 2.5GBase-T mode on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. if auto-negotiated/forced to 100/1000MBase-T on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off - No link
Right Activity/POE LED: Green/Amber
Flashing Green (~30ms) = Port Activity and POE Power Off. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity and POE Power ON Amber (Luminance at 1.5ft =180+10 cd/m2)
Solid Amber =No Port Activity and POE Power ON. Amber (Luminance at 1.5ft = 45+5 cd/m2)

Off = No activity and POE Power Off

N2224X RJ45 port status LED Indications

Left Link/Speed LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. if auto-negotiated/forced to 2.5GBase-T mode on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. if auto-negotiated/forced to 100/1000MBase-T on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off - No link
Right Activity LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

QSFP port status LED Indications

1st LED: Green
Solid Green = Port linked. Green (Luminance at 1.5ft =45+5 cd/m2)
Off = No Link
2nd LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

SFP28 port status LED Indications

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 25GE on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. lower than 25GE on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No Link
2nd LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

N2248X-ON/N2248PX-ON Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – all functions are normal. • Flashing Green – Booting. • Solid Amber –Major Fault. Indicates summary of all major faults within the system; the faults are traffic affecting. • Flashing Amber –Minor Fault: Indicates summary of all minor faults within the system; the faults are not traffic affecting.	At front side
Power LED	• Solid Green – Normal. • Solid Amber – POST in progress. • Flashing Amber – Power supply fault. • Off – No power.	At front side
FAN LED	• Solid Green – all functions are normal. • Solid Amber –Any Fan tray fault.	At front side
Beacon LED	Not in use.	At front side
Stacking LED	Not in use.	At front side
7-DIGIT Stack LED	Not in use.	At front side

Port LED Definition

N2248PX RJ45 port status LED Indications

Left Link/Speed LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. if auto-negotiated/forced to 2.5GBase-T mode on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. if auto-negotiated/forced to 100/1000MBase-T on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off - No link
Right Activity/POE LED: Green/Amber
Flashing Green (~30ms) = Port Activity and POE Power Off. Green (Luminance at 1.5ft = 45+5 cd/m2)
Flashing Amber (~30ms) =Port Activity and POE Power ON Amber (Luminance at 1.5ft =180+10 cd/m2)
Solid Amber =No Port Activity and POE Power ON. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity and POE Power Off

N2248X RJ45 port status LED Indications

Left Link/Speed LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. if auto-negotiated/forced to 2.5GBase-T mode on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. if auto-negotiated/forced to 100/1000MBase-T on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off - No link
Right Activity LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

QSFP port status LED Indications

1st LED: Green
Solid Green = Port linked. Green (Luminance at 1.5ft =45+5 cd/m2)
Off = No Link
2nd LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

SFP28 port status LED Indications

1st LED: Green/Amber
Solid Green = Port linked operating at max port speed, i.e. running 25GE on the port. Green (Luminance at 1.5ft = 45+5 cd/m2)
Solid Amber = Port linked operating at lower speed, i.e. lower than 25GE on the port. Amber (Luminance at 1.5ft = 45+5 cd/m2)
Off = No Link
2nd LED: Green
Flashing Green (~30ms) = Port Activity. Green (Luminance at 1.5ft = 45+5 cd/m2)
Off = No activity

EdgeCore/Accton Switches

- AS4610 Serial Switch
- AS4625-54P/AS4625-54T Switch
- AS4630-54NPE Switch
- AS7816-64X Switch
- AS5835-54X Switch
- AS4630-54PE Switch
- AS5712-54X Switch
- AS9716-32D Switch
- AS7312-54X/AS7312_54XS Switch
- AS5812-54T Switch
- AS5812-54X Switch
- AS5835-54T Switch
- AS6712-32X Switch
- AS6812_32X Switch
- AS7326-56X Switch
- AS7712-32X Switch
- AS7726-32X Switch

AS4610 Serial Switch

As4610 serial includes as4610-54p, as4610-30p, as4610-54t, as4610-54t_B.

·System LED Definition：

LED	Condition	Status
System	Green solid	System Diagnostic & OS OK
	Green Blinking	System Diagnostic & OS in progress
	Amber solid	System Diagnostic & OS Failed
PSU1	Green solid	Power supply 1 operates normally
	Amber solid	Power supply 1 present but fault
	Off	Power supply 1 isn't presented. No PSU1
PSU2	Green solid	Power supply 2 operates normally
	Amber solid	Power supply 2 present but fault
	Off	Power supply 2 isn't presented. No PSU2
FAN	Green solid	Fan works normally
	Amber solid	Fan fail
PoE	Green solid	System has power budget for PoE.
	Amber solid	System doesn't have power budget for PoE.
STK1	Not supported.	
STK2	Not supported.	
PRI	Not supported.	

·port LED Definition：

Port Type	Condition	Status
RJ-45 Port	Green	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber	Port Link with POE
	Amber Blinking	Port Link/Activity with POE
SFP+ Port	Green	10G Port Link
	Green Blinking	10G Port Link/Activity
	Amber	1G Port Link
	Amber Blinking	1G Port Link/Activity
	Off	No Link
QSFP Port	Green	20G Port Link
	Green Blinking	20G Port Link/Activity
	Off	No Link

AS4625-54P/AS4625-54T Switch

System LED Definition

LED	Condition	Status
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green –System diagnostic & OS in progress • Solid Amber –System diagnostic & OS Failed	At front
PSU1/PSU2 LED (Bi-color LED)	• Green – Normal • Amber –PSU1/PSU2 present but PG fail • Off – No main power supply present	At front
FAN Status LED (Bi-color LED)	• Green –Fan is OK • Amber – Fan tray fault • Off – The sku doesn't have system fan	At front
Location LED	Not supported.	At front
PoE LED (Only for AS4625-54P)	• Green – PoE loading << power budget • Amber –PoE loading ~ power budget • Off – None PoE sku	At front

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
1~48 Port	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP+ port status LED Indications

LED	Condition	Status
(Link/Activity) 49~54 Ports	Green Solid	Port Link on 10G mode
	Green Blinking	Port Link/Activity on 10G mode
	Amber Solid	Port Link on 1G mode
	Amber Blinking	Port Link/Activity on 1G mode

OOB Ethernet Port LEDs:

LED	Description
Link LED	• Solid green –The port is Link Up • Off –The port is Link Down
Activity LED	• Off – The port is no activity • Flashing Green – Activity

AS4630-54NPE Switch

System LED Definition

LED	Condition	Status
System LED	Green solid	System Diagnostic & OS OK.
	Green Blinking	System Diagnostic & OS in progress.
	Amber solid	System Diagnostic & OS Failed.
PSU1 LED	Green solid	Power supply 1 operates normally.
	Amber solid	Power supply 1 present but fault.
	Off	Power supply 1 isn't presented. No PSU1.
PSU2 LED	Green solid	Power supply 2 operates normally.
	Amber solid	Power supply 2 present but fault.
	Off	Power supply 2 isn't presented. No PSU2.
FAN LED	Green solid	Fan works normally.
	Amber solid	Fan fails.
	Off	The SKU doesn't have system fan.
PoE LED	Green solid	PoE loading << power budget.
	Amber solid	PoE loading ~ power budget.
	Off	None PoE sku.
STK1/STK2 LED	Not in use.	
PRI LED	Not in use.	

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
1~48 Port	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 49~52 Ports	White solid	Port Link on 25G mode
	White Blinking	Port Link/Activity on 25G mode
	Green solid	Port Link on 10G mode
	Green Blinking	Port Link/Activity on 10G mode

QSFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 53~54 Ports	White solid	Port Link on 100G mode
	White Blinking	Port Link/Activity on 100G mode
	Green solid	Port Link on 40G mode

	Green Blinking	Port Link/Activity on 40G mode

AS7816-64X Switch

System LED Definition

Feature	Detailed Description	Comment
Power Supply 1	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
Power Supply 2	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
FANs	• Red –Error/Failure/Bad • Green –Good	At front
Diag	• Red –Error/Failure/Bad • Green –Good • Blinking Green –System boot in progress	At front
LOC	Not supported.	At front

Port LED Definition

Feature	Detailed Description
LED 1	• Blue – Link at 100Gbps (4 x 25G) • Orange– Link at 40Gbps (4 x 10G) • White– 25G • Green– 10G • OFF –not present
LED 2~4	• White– 25G • Green– 10G • OFF –not present

Management Port LED

Feature	Detailed Description
LED	• Off –not present • Green – Link at 10/ 100M /1000M • Toggle – Activity

Console port LED:

Feature	Detailed Description
LED	• Off – No Link • Solid green – Link is present

AS5835-54X Switch

·System LED Definition：

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

·port LED Definition：

LED	Condition	Status
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	SFP+ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 100G Mode (Port 49~ 54)	On/Flashing Green	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 25G Mode (With Breakout cable)	On/Flashing Amber	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 40G Mode	On/Flashing	QSFP port has a valid link at 100G.

(Port 49~ 54)	blue	Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 10G Mode (With Breakout cable)	On/Flashing purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present.OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 10G SFP+ and 40/100G QSFP28 uplink port to indicate link/activity.
- There should be four LEDs per QSFP28 port. These LEDs can represent state of 40/100GE port or 4 10/25GE ports when used in breakout mode.
- The 40/100G QSFP28 LED should present OFF while there’s breakout cable plugged in.

AS4630-54PE Switch

System LED Definition

LED	Condition	Status
System LED	Green solid	System Diagnostic & OS OK
	Green Blinking	System Diagnostic & OS in progress
	Amber solid	System Diagnostic & OS Failed
PSU1 LED	Green solid	Power supply 1 operates normally
	Amber solid	Power supply 1 present but fault
	Off	Power supply 1 isn't presented. No PSU1
PSU2 LED	Green solid	Power supply 2 operates normally
	Amber solid	Power supply 2 present but fault
	Off	Power supply 2 isn't presented. No PSU2
FAN LED	Green solid	Fan works normally
	Amber solid	Fan fail
	Off	The SKU doesn't have system fan.
PoE LED	Green solid	PoE loading << power budget
	Amber solid	PoE loading ~ power budget
	Off	None PoE sku.
STK1/STK2 LED	Not in use.	
PRI LED	Not in use.	

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
0~47 Port (1~48)	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 49~52 Ports	Green solid	Port Link on 25G mode
	Green Blinking	Port Link/Activity on 25G mode
	White solid	Port Link on 10G mode
	White Blinking	Port Link/Activity on 10G mode
	Off	Link down

QSFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 53~54 Ports	White solid	Port Link on 100G mode
	White Blinking	Port Link/Activity on 100G mode

	Green solid	Port Link on 40G mode
	Green Blinking	Port Link/Activity on 40G mode
	Off	Link down

AS5712-54X Switch

·System LED Definition：

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

·port LED Definition：

LED	Condition	Status
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	SFP+ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 40G Mode (Port 49~ 54)	On/Flashing Green	SFP+ port has a valid link at 40G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 10G Mode (With Breakout cable)	On/Flashing Amber	QSFP port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40G QSFP+ uplink port to indicate link/activity.
- There should be four LEDs per QSFP port. These LEDs can represent state of 40GE port or 4 10GE ports when used in breakout mode.
- The 40G QSFP+ LED should present OFF while there’s breakout cable plugged in.

AS9716-32D Switch

System LED Definition

Feature	Detailed Description	Comment
Diagnosis LED	• Solid green – All OK, CLI prompt available • Blinking green – Boot-up in progress • Solid amber –System self-diagnostic test has detected a fault (Fan, thermal or any interface fault.).	At front
FAN LED	• Solid green –System FAN operating normally. • Solid amber –Fan tray present buy system FAN is fault. • OFF – System OFF.	At front
PS1 LED	• Solid green –This power is operating normally. • Solid amber –PWR present but not power on or this power is fault. • OFF – Power supply not present.	At rear
PS2 LED	• Solid green –This power is operating normally. • Solid amber –PWR present but not power on or this power is fault. • OFF – Power supply not present.	At front
Locator LED	Not supported.	At front

Port LED Definition

QSFP56-DD ports LED Indications

Only the 1st LED is used when running at 400G without breakout.
Solid Blue - Port linked operating at max port speed 400G.
Off - No link
Flashing Blue - Transmit/Receive is activity.
Only the 1st LED is used when running at 100G without breakout.
Solid Green - Port linked operating at max port speed 100G.
Off - No link
Flashing Green - Transmit/Receive is activity.
All four LEDs are used when running at 4 x100G in breakout mode.
Solid Green - Port linked operating at max port speed 100G
Off - No link
Flashing Green -Transmit/Receive is activity

Management Port LED SFP+

Feature	Detailed Description
SFP+ 10G management port LED	• Off – No Link • On/Flashing Green –SFP+ port has a valid link at 10G. Flashing indicates activity. • On/Flashing Amber –SFP+ port has a valid link at 1G. Flashing indicates activity.
RJ45 10/100/1G Management port LED	• Off – No Link • On/Flashing Green –Has a valid link. Flashing indicates activity.

AS7312-54X/AS7312_54XS Switch

System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

port LED Definition

LED	Condition	Status
SFP28 Port LED	On/Flashing Green	SFP28 port has a valid link at 25G. Flashing indicates activity.
	On/Flashing Amber	SFP28 port has a valid link at 10G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 100G Mode(Port 49~ 54)	On/Flashing Green	QSFP28 port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 25G Fan Out Mode (With Breakout cable)	On/Flashing Red	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 40G Mode (Port 49~ 54)	On/Flashing Blue	QSFP28 port has a valid link at 40G. Flashing indicates activity.

	Off	There is no link on the port.
QSFP28 Port LED in 10G Fan Out Mode (With Breakout cable)	On/Flashing Red	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

AS5812-54T Switch

System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

port LED Definition

LED	Condition	Status
1~48 Port LED	On/Flashing Green	Port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	Port has a valid link at 1G/100M. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 40G Mode (Port 49~ 54)	On/Flashing Green	SFP+ port has a valid link at 40G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 10G Mode (With Breakout cable)	On/Flashing Green	QSFP port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.

	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40G QSFP+ uplink port to indicate link/activity.
- There should be four LEDs per QSFP port. These LEDs can represent state of 40GE port or 4 10GE ports when used in breakout mode.
- The 40G QSFP+ LED should present OFF while there’s breakout cable plugged in.

AS5812-54X Switch

·System LED Definition：

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

·port LED Definition：

LED	Condition	Status
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	SFP+ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 40G Mode (Port 49~ 54)	On/Flashing Green	SFP+ port has a valid link at 40G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 10G Mode (With Breakout cable)	On/Flashing Green	QSFP port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link

	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40G QSFP+ uplink port to indicate link/activity.
- There should be four LEDs per QSFP port. These LEDs can represent state of 40GE port or 4 10GE ports when used in breakout mode.
- The 40G QSFP+ LED should present OFF while there’s breakout cable plugged in.

AS5835-54T Switch

System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

Port LED Definition

LED	Condition	Status
1~48 Port LED	On/Flashing Green	RJ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	RJ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 100G Mode (Port 49~ 54)	On/Flashing Green	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 25G Mode (With Breakout cable)	On/Flashing Amber	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 40G Mode (Port 49~ 54)	On/Flashing blue	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 10G Mode (With Breakout cable)	On/Flashing purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP

		end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40/100G QSFP28 uplink port to indicate link/activity.
- There should be four LEDs per QSFP28 port. These LEDs can represent state of 40/100GE port or 4 10/25GE ports when used in breakout mode.
- The 40/100G QSFP28 LED should present OFF while there’s breakout cable plugged in.

AS6712-32X Switch

·System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Orange	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Orange	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Orange	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Orange	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

Port LED Definition

LED	Condition	Status
QSFP+ Port LED	On/Flashing Green	QSFP port has a valid link at 40G. Flashing indicates activity.
	On/Flashing Orange	QSFP port has a valid link at 10G via break out cable. Flashing indicates activity.
	Off	There is no link on the port.
Management Port LED (Link)	On Green	Port has a valid link
	Off	There is no link on the port
Management Port LED (Activity)	Flashing Green	Flashing indicates activity

	Off	There is no link on the port

AS6812_32X Switch

System LED Definition

LED	Color	Status
Power Supply 1	Green	This power is operating normally.
	Orange	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Power Supply 2	Green	This power is operating normally.
	Orange	PWR present but not power on or this power is fault.
	Off	Power supply not present.
FAN	Green	System FAN operating normally.
	Orange	Fan tray present by system FAN is fault.
	Off	System OFF
Diag	Green	System self-diagnostic test successfully completed.
	Orange	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
LOC	Not supported.	

Port LED Definition

LED	Condition	Status
QSFP+ Port LED	On/Flashing Orange	QSFP port has a valid link at 40G. Flashing indicates activity.
	On/Flashing Green	QSFP port has a valid link at 10G via breakout cable. Flashing indicates activity.
	OFF	There is no link on the port.
Management Port LED (Link)	On Green	Port has a valid link
	Off	There is no link on the port
Management Port LED (Activity)	Flashing Green	Flashing indicates activity

AS7326-56X Switch

System LED Definition

LED	Color	Mode
Power Supply 1	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
Power Supply 2	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
FANs	Red	Error/Failure/Bad
	Green	Good
Diag	Red	Error/Fault/Failure
	Green	Good
	Blinking Green	System boot in progress
LOC	Not supported.	

Port LED Definition

SFP28 Port LED Definition

LED	Color	Mode
SFP28 Port LED	On/Flashing Green	SFP28 port has a valid link at 25G. Flashing indicates activity.
	On/Flashing Yellow	SFP28 port has a valid link at 10G. Flashing indicates activity.
	OFF	There is no link on the port.

QSFP28 Port LED Definition

LED	Color	Mode
LED 1~4 (Port 49~56)	On/Flashing Green	QSFP28 port has a valid link at 100G. Flashing indicates activity.
	OFF	There is no link on the port.
	On/Flashing Blue	QSFP28 port has a valid link at 40G. Flashing indicates activity.
	OFF	There is no link on the port.

	On/Flashing Yellow	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity. (With Breakout cable)
	OFF	There is no link on the port.
	On/Flashing Purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity. (With Breakout cable)
	OFF	There is no link on the port

SFP+ Port LED Definition

LED	Color	Mode
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Yellow	SFP+ port has a valid link at 1G. Flashing indicates activity.
	OFF	There is no link on the port.

Management Port LED

LED	Color	Mode
MGMT Port LED	On Green	Port has a valid link
	Flashing Yellow	Flashing indicates activity
	OFF	There is no link on the port.

AS7712-32X Switch

System LED Definition

LED	Color	Mode
Power Supply 1	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
Power Supply 2	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
FANs	Red	Error/Failure/Bad
	Green	Good
Diag	Red	Error/Fault/Failure
	Green	Good
	Blinking	System boot in progress
	Green	
LOC	Not supported.	
System	Not supported.	

Management Port LED Definition

LED	Color	Mode
LED	Green	10/ 100M /1000M
	Toggle	Activity
	off	not present

Port LED Definition

LED	Color	Mode
LED 1	Blue	100G (4 x 25G)
	Orange	40G (4 x 10G)
	White	25G

	Green	10G
	off	not present
LED 2~4	White	25G
	Green	10G
	off	not present

AS7726-32X Switch

System LED Definition

Feature	Detailed Description	Comment
Power Supply 1	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
Power Supply 2	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
FANs	• Red –Error/Failure/Bad • Green –Good	At front
Diag	• Red –Error/Failure/Bad • Green –Good • Blinking Green –System boot in progress	At front
LOC	Not supported.	At front

Port LED Definition

Feature	Detailed Description
LED 1	• Blue – Link at 100Gbps (4 x 25G) • Orange– Link at 40Gbps (4 x 10G) • White– 25G • Green– 10G • OFF –not present
LED 2~4	• White– 25G • Green– 10G • OFF –not present

Management Port LED

The management port support 1G/ 100M / 10M speed. Only the right port LED is in use.

Feature	Detailed Description
LED	• Off –not present • Yellow – Link at 10/ 100M /1000M

Delta/Agema Switches

- AG9032v1 Switch
- AG5648V1 Switch
- AG7648 Switch

AG9032v1 Switch

·System LED Definition：

Feature	Detailed Description	Comment
Power 1 LED	• Solid Green – Power Supplier 1 is supplied to the switch & operating normally • Blinking Amber – Power Supplier 1 failed. • Off – Power is Disconnected.	At front
Power 2 LED	• Solid Green – Power Supplier 2 is supplied to the switch & operating normally. • Blinking Amber – Power Supplier 2 failed. • Off – Power is Disconnected.	At front
System LED	• Solid Green – Normal operation • Blinking Green – Booting progress • Solid Red – System is failed • Off – No Power	At front
FAN Status LED	• Solid Green – FAN operating normally. • Solid Amber – FAN failed.	At front
Management (RJ-45) Two LEDs /port	Link LED: (on the left side) • Off – No link is established on the port. • Solid Yellow – A valid link at 10/100Mbps is established on the port. • Solid Green – A valid link at 1000Mbps is established on the port. Act LED: (on the right side) • Off – No link is established on the port. • Blinking green – Activity, transmitting or receiving packet at this port.	At front
PSU LED	• Solid green – Good AC input. • Solid red – NO AC input.	At rear
FAN Status LED	• Green – FAN operating normally. • Red – FAN failed.	At rear

⚠ For FAN LED , when one of FAN LEDs on the rear side failed , fan led on the front panel will display amber.

·port LED Definition：

Feature	Detailed Description
LED 1	• Green 100G operation • Amber 40G operation • Blue 25G operation • Purple 10G operation • Off No Link
LED 2	Working in breakout only. • Blue 25G operation • Purple 10G operation • Off 40G/100G operation (Assuming LED 1 is illuminated) or No Link
LED 3	Working in breakout only. • Blue 25G operation • Purple 10G operation • Off 40G/100G operation (Assuming LED 1 is illuminated) or No Link
LED 4	Working in breakout only. • Blue 25G operation • Purple 10G operation • Off 40G/100G operation (Assuming LED 1 is illuminated) or No Link
NOTE: Off: No Link Solid: Linkup Flashing: Traffic	

AG5648V1 Switch

System LED Definition：

Label	Detailed Description	Comment
System LED	• Solid Green – Operating • Blinking Green – Booting or System in Diagnostic mode • Solid Amber – Critical Alarm • Off – Power is Disconnected	At front side
Power LED	• Solid Green –2 Power Suppliers are supplied to the switch & operating normally • Solid Amber –Booting or Single power supplier is installed/operating. • Blinking Amber –2 Power Suppliers are installed, but only single power supply is operating. • Off – Power is Disconnected.	At front side
FAN LED	• Solid Green – FAN operating normally. • Solid Amber – A FAN or more failed	At front side

Note:

For FAN LED, when one of FAN LEDs on the rear side failed, fan led on the front panel will display Amber

QSFP28 port LEDs

LED	Detailed Description
Link/ACT LED	• OFF –No link is established on the port. • Solid Green – A valid link is established as 100GE on the port. • Solid Amber – A valid link is established as 40GE on the port. • Solid Blue – A valid link is established as 25GE on the port. (Through break out cable) • Solid Purple –A valid link is established as 10GE on the port. (Through break out cable) • Blinking LED – Packets transmission or reception is occurring

SFP28 port LEDs：

LED	Detailed Description
Link/ACT LED	• OFF –No link is established • Two LEDs / Port Solid Green – A valid 25G link is established • Solid Yellow – A valid 10G link is established • Blinking LED – Packets transmission or reception is occurring

OOB Management Ethernet port LEDs

LED	Detailed Description
Link LED	• Solid Green = Port linked operating at max port speed, i.e. if auto-negotiated/forced to 1G mode • Solid Amber = Port linked operating at lower speed, i.e. if auto-negotiated/forced to 10/100M on this port • Off = No Link
Activity	• Flashing Green (~30ms) = Port Activity • Off = No activity

AG7648 Switch

System LED Definition

Feature	Detailed Description	Comment
System LED	• Solid green – All OK, CLI prompt available • Blinking green – Boot-up in progress • Solid yellow – Major Fault. Displays summary of all major faults within the system; the faults are traffic affecting. • Blinking yellow – Minor Fault: Displays summary of all minor faults within the system; the faults are not traffic affecting.	At front
FAN LED	• Solid green –fan powered and @expected rpm • Solid yellow –fan failed including incompatible airflow direction from what is indicated in the Board ID for the particular SKU.	At front
PSU LED	• Solid green – The DC output is on and OK. • Solid yellow– Power supply critical event causing a shutdown; failure, OCP, OVP, Fan Fail, OTP, UVP. • Blinking yellow–Power supply warning events where the power supply continues to operate; high temp (PMBus reading inlet > 60deg; PMBus reading hotspot > 100deg), high power, high current (105 %*), slow fan.	At rear
Power LED	• Off - No power • Solid Yellow - POST in progress • Solid Green - Normal Operation (dual or single supply) • Blinking Yellow - One of Power Supplier is failed	At front
LOCATOR LED	Not supported.	At front

Port LED Definition

SFP+ port LEDs

Feature	Detailed Description
Link LED	• Off – No Link • Solid green – Link on 10G speed • Solid amber – Link on 1G speed
Activity LED	• Off – No Link • Blinking green – Transmit/Receive is activity

QSFP+ port LEDs

Feature	Detailed Description
Link/ACT LED	• Off – No Link • Solid green – Link on 40G speed • Solid Amber- Link on 10G speed • Blinking green – 40G speed, transmit/Receive is activity • Blinking amber – 10G speed, transmit/Receive is activity

Front Management Ethernet port LEDs

Feature	Detailed Description
Link LED	• Off – No Link • Solid green – Link on 1G speed • Solid yellow – Link on 10M/100M speed
Activity LED	• Off – No Link • Blinking green – Transmit/Receive is activity

FS Switches

- N5850-48S6C Switch
- N8550-32C Switch
- N5850-48S6Q Switch
- S5810-48TS-P Switch
- S5810-28FS Switch
- S5810-28TS Switch
- S5810-48FS Switch
- S5810-48TS Switch
- S5860-20SQ Switch
- S5860-24XB-U Switch
- N8560-32C Switch
- N8560-64C Switch
- S5860-24MG-U Switch
- S5860-48XMG-U Switch
- S5860-24XMG Switch
- S5860-48MG-U Switch
- S5860-48XMG Switch
- S5870-48T6S/S5870-48T6S-U Switch
- S5870-48T6BC/S5870-48T6BC-U Switch
- N5850-48X6C Switch
- N8550-64C Switch
- N9550-32D Switch
- S5870-48MX6BC-U Switch
- S3410-24TS Switch
- S3410L-24TF Switch
- S3410L-24TF-P Switch
- S3410-24TS-P Switch
- S3410C-8TMS-P Switch
- S3410C-16TF Switch
- S3410C-16TMS-P Switch
- S3410C-16TF-P Switch
- S3410-48TS-P Switch
- N8550-48B8C Switch
- S3410-48TS Switch
- S3410L-48TF Switch
- N8550-24CD8D Switch
- N9600-64OD Switch

N5850-48S6C Switch

System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

port LED Definition

LED	Condition	Status
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	SFP+ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 100G Mode (Port 49~ 54)	On/Flashing Green	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 25G Mode (With Breakout cable)	On/Flashing Amber	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 40G Mode	On/Flashing blue	QSFP port has a valid link at 100G. Flashing indicates activity.

(Port 49~ 54)	Off	There is no link on the port.
QSFP28 Port LED in 10G Mode (With Breakout cable)	On/Flashing purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 10G SFP+ and 40/100G QSFP28 uplink port to indicate link/activity.
- There should be four LEDs per QSFP28 port. These LEDs can represent state of 40/100GE port or 4 10/25GE ports when used in breakout mode.
- The 40/100G QSFP28 LED should present OFF while there’s breakout cable plugged in.

N8550-32C Switch

System LED Definition

Feature	Detailed Description	Comment
Power Supply 1	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
Power Supply 2	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
FANs	• Red –Error/Failure/Bad • Green –Good	At front
Diag	• Red –Error/Failure/Bad • Green –Good • Blinking Green –System boot in progress	At front
LOC	Not supported.	At front

Port LED Definition

Feature	Detailed Description
LED 1	• Blue – Link at 100Gbps (4 x 25G) • Orange– Link at 40Gbps (4 x 10G) • White– 25G • Green– 10G • OFF –not present
LED 2~4	• White– 25G • Green– 10G • OFF –not present

Management Port LED

The management port support 1G/ 100M / 10M speed. Only the right port LED is in use.

Feature	Detailed Description
LED	• Off –not present

	• Yellow – Link at 10/ 100M /1000M

N5850-48S6Q Switch

·System LED Definition：

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

·port LED Definition：

LED	Condition	Status
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	SFP+ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 40G Mode (Port 49~ 54)	On/Flashing Green	SFP+ port has a valid link at 40G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP+ Port LED in 10G Mode (With Breakout cable)	On/Flashing Green	QSFP port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.

OOB LED (Link)	On	Port has a valid link
	Off	There is no link on the port
OOB LED (Activity)	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40G QSFP+ uplink port to indicate link/activity.
- There should be four LEDs per QSFP port. These LEDs can represent state of 40GE port or 4 10GE ports when used in breakout mode.
- The 40G QSFP+ LED should present OFF while there’s breakout cable plugged in.

S5810-48TS-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	1. System (including any module) Failure 2. The temperature of any part of the machine exceeds 60ºC.
PS1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PS2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
PoE LED (controlled by PoE button on the front panel)	Solid green	Port LEDs indicate switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

NOTE:

PoE button

The 48x1G RJ45 ports on the front panel support PoE.

PoE button on the front panel controls whether the port LED indicates data switching status or PoE power supply status of the first 48 ports.

- By default, port LED indicates data switching status of the port. PoE LED on the front panel of system LED block is solid green.
- If pressed the PoE button, the port LED indicates PoE power supply status of the port. PoE LED on the front panel of system LED block changes to solid amber.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On • Off –PoE Power Off

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S5810-28FS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	1. System (including any module) Failure 2. The temperature of any part of the machine exceeds 60ºC.
PS1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PS2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

Port LED Definition

10/100/1000BASE-T RJ45 port (Combo) LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port (Combo) LED	• Off – No Link • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.

GE SFP port

Feature	Detailed Description
GE SFP port LED	• Off – No Link • Solid Green –Port links up at 1000M.

	• Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S5810-28TS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	1. System (including any module) Failure 2. The temperature of any part of the machine exceeds 60ºC.
PS1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PS2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

Port LED Definition

10/100/1000BASE-T RJ45 port LED and combo port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED and combo port LED	• Off – No Link • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.

GE SFP port

Feature	Detailed Description
GE SFP port LED	• Off – No Link • Solid Green –Port links up at 1G.

	• Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S5810-48FS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking Green	Boot-up in progress.
	Solid Green	The system completes initialization and works normally.
	Solid Amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid Red	1. System (including any module) Failure 2. The temperature of any part of the machine exceeds 60ºC.
PS1 LED	OFF	Power supply not present.
	Solid Green	This power is operating normally.
	Solid Red	Power module failure or need to connect to the AC power line.
	Solid Amber	1. Power mixing that does not support mixing appears; 2. The model number can be read, but the model is not recognized; 3. The power supply is not powerful enough to power up the newly inserted expansion card or low priority expansion card.
PS2 LED	OFF	Power supply not present.
	Solid Green	This power is operating normally.
	Solid Red	Power module failure or need to connect to the AC power line.
	Solid Amber	1. Power mixing that does not support mixing appears; 2. The model number can be read, but the model is not recognized; 3. The power supply is not powerful enough to power up the newly inserted expansion card or low priority expansion card.
MGMT LED	OFF	No Link.
	Solid Green	Port linked operating at 1000M.
	Solid Amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

Port LED Definition

GE SFP port LED

Feature	Detailed Description
GE SFP port LED	• Off – No Link • Solid Green –Port links up at 1G.

	• Flashing –Transmit/Receive is activity.

10G SFP+ port LED

Feature	Detailed Description
10G SFP+ port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S5810-48TS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	1. System (including any module) Failure 2. The temperature of any part of the machine exceeds 60ºC.
PS1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PS2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – No Link • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G.

	• Flashing –Transmit/Receive is activity.

S5860-20SQ Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	A: Boot-up in progress; B: Short pressing the reset button starts flashing, and after collecting system information, it will return to normal light.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold
	Solid red	1. System Failure A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
	Blinking red	A. Long pressing the reset button, it will flash green for the first 5S, and then flash red until the information is collected and the whole machine is reset. B. An optical module short-circuit fault occurs; (see CPLD register)
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system B. The actual speed read is less than 3000 rpm (judged as stalled). C. Fan power_ok abnormality (see CPLD register) 2. Any fan is not in position (see CPLD register);
PS1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	1. Power module failure. A. Cannot read the model number of the power supply module. B. Can read the model number, but does not match the system 2. Power supply appears PWR_ALARM (see CPLD register)
PS2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	1. Power module failure. A. Cannot read the model number of the power supply module. B. Can read the model number, but does not match the system 2. Power supply appears PWR_ALARM (see CPLD register)

MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
ID LED	OFF	Location function is disabled.
	Solid blue	Location function is enabled. Used to locate switches, O&M personnel can remotely control ID lights on and off.

Port LED Definition

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • On/Flashing Green –SFP+ port has a valid link at 10G or 1G. Flashing indicates activity.
SFP28 25G port LED	• Off – No Link • On/Flashing Green –SFP28 port has a valid link at 25G, 10G or 1G. Flashing indicates activity.
QSFP+ 40G port LED	1st LED: Green/OFF • On/Flashing Green = Port linked operating at 40G. Flashing indicates activity. • Off – No Link • All four LEDs shall be used when 4 x10G or 4 x1G mode is running on QSFP+ port. • On/Flashing Green = Port linked operating at 4x10G or 4 x1G. Flashing indicates activity. • Off – No Link

S5860-24XB-U Switch

System LED Definition

LED Name	Status	Detailed Description
System LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold 2. Power mixing
	Solid red	1. System Failure A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
	Blinking red	A. Long pressing the reset button, it will flash green for the first 5S, and then flash red until the information is collected and the whole machine is reset. B. An optical module short-circuit fault occurs; (see CPLD register)
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system B. The actual speed read is less than 3000 rpm (judged as stalled). C. Fan power_ok abnormality (see CPLD register) 2. Any fan is not in position (see CPLD register);
PS LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	A. Power module failure, no output of 12V, 54V B. Power module not connected to AC power cord C. Cannot read the model number of the power supply module. D. Can read the model number, but does not match the system
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
PoE LED (controlled by PoE button on	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

the front panel)		

Port LED Definition

RJ45 100M/1G/2.5G/5G/10G port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link • Solid Green –Port links up at 1G/2.5G/5G/10G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On • Off –PoE Power Off • Solid Amber –Port PoE overload or failure

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link • Solid Green –Port links up at 1G/10G/25G. • Flashing –Transmit/Receive is activity.

N8560-32C Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Boot-up in progress. 2. The main BIOS flash boot failure. 3. If the main BMC flash boot failure, backup BMC boot success.
	Blinking amber	1. Both of the main BMC and backup BMC flash boot failure. 2. Both of the main BIOS and backup BIOS flash boot failure.
PSU LED	Solid green	This power is operating normally.
	Solid amber	Power module failure or DC operating abnormally.
FAN LED	Solid green	Fan operating normally.
	Solid amber	Fan failed.

Port LED Definition

Feature	Detailed Description
100G QSFP28 port LED	• Off – No Link • Solid Green –Port links up at 100G. • Solid Amber –Port links up at the speed lower than 100G. • Flashing –Transmit/Receive is activity.

N8560-64C Switch

System LED Definition

LED Name	Status	Detailed Description
SYS LED	OFF	No power supply.
	Solid green	The system completes initialization and works normally.
	Blinking green	The system is initializing.
PSU LED (front panel)	OFF	No power supply inserted.
	Blinking red	Only one power supply inserted.
	Solid green	Two power supplies are operating normally.
	Solid amber	Power module failure or DC operating abnormally.
FAN LED (front panel)	OFF	No fan inserted.
	Solid green	Fan operating normally.
	Solid amber	Fan failed.
PSU LED (rear panel)	OFF	No power supply inserted
	Solid green	This power is operating normally.
	Solid amber	Power module is inserted but not powered on.
FAN LED (rear panel)	OFF	No fan inserted.
	Blinking green	Fan operating normally.
	Solid amber	Fan failed.
LCT LED	OFF	Location function is disabled.
	Solid blue	Location function is enabled. The O&M personnel is locating switches.
BMC LED	Not supported.	

Port LED Definition

Feature	Detailed Description
40G/100G QSFP28 port LED	• Off – No Link. • Solid Green –Port links up at 100G.

	• Solid Amber –Port links up at 40G. • Flashing –Transmit/Receive is activity.

S5860-24MG-U Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold. 2. Power mixing.
	Solid red	1. System Failure. A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
LED Mode LED (controlled by LED Mode button on the front panel)	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

RJ45 100M/1G/2.5G/5G port LED

Feature	Detailed Description
Non-PoE (controlled by LED Mode button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1G/2.5G/5G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by LED Mode button on the front panel)	• Solid Green –PoE Power On. • Off –PoE Power Off. • Solid Amber –Port PoE overload or failure.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link. • Solid Green –Port links up at 1G/10G/25G. • Flashing –Transmit/Receive is activity.

S5860-48XMG-U Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold. 2. Power mixing.
	Solid red	1. System Failure. A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system. B. The actual speed read is less than 3000 rpm (judged as stalled). C. Fan power_ok abnormality. 2. Any fan is not in position (see CPLD register);
PWR LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	A. Power module failure, no output of 12V, 54V. B. Power module not connected to AC power cord. C. Cannot read the model number of the power supply module. D. Can read the model number, but does not match the system.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
LED Mode LED	Solid green	Port LEDs indicate data switching status.

(controlled by LED Mode button on the front panel)	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

RJ45 100M/1G/2.5G/5G/10G port LED

Feature	Detailed Description
Non-PoE (controlled by LED Mode button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1G/2.5G/5G/10G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by LED Mode button on the front panel)	• Solid Green –PoE Power On. • Off –PoE Power Off. • Solid Amber –Port PoE overload or failure.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link. • Solid Green –Port links up at 25G. • Flashing –Transmit/Receive is activity.

QSFP+ 40G port LED

Feature	Detailed Description
QSFP+ 40G port LED	• Off – No Link. • Solid Green –Port links up at 40G. • Flashing –Transmit/Receive is activity.

S5860-24XMG Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold 2. Power mixing
	Solid red	1. System Failure A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system B. The actual speed read is less than 3000 rpm (judged as stalled). C. Fan power_ok abnormality 2. Any fan is not in position (see CPLD register);
PWR LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	A. Power module failure, no output of 12V, 54V B. Power module not connected to AC power cord C. Cannot read the model number of the power supply module. D. Can read the model number, but does not match the system
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.
LED Mode LED	Not in use.	

Port LED Definition

RJ45 100M/1G/2.5G/5G/10G port LED

Feature	Detailed Description
RJ45 100M/1G/2.5G/5G/10G port LED	• Off – No Link • Solid Green –Port links up at 1G/2.5G/5G/10G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link • Solid Green –Port links up at 1G/10G/25G. • Flashing –Transmit/Receive is activity.

S5860-48MG-U Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold 2. Power mixing
	Solid red	1. System Failure A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system B. The actual speed read is less than 3000 rpm (judged as talled). C. Fan power_ok abnormality 2. Any fan is not in position (see CPLD register);
PWR LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	A. Power module failure, no output of 12V, 54V. B. Power module not connected to AC power cord. C. Cannot read the model number of the power supply module. D. Can read the model number, but does not match the system.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

LED Mode LED (controlled by LED Mode button on the front panel)	Solid green	Port LEDs indicate data switching status.
	olid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

RJ45 100M/1G/2.5G/5G port LED

Feature	Detailed Description
Non-PoE (controlled by LED Mode button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1G/2.5G/5G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by LED Mode button on the front panel)	• Solid Green –PoE Power On. • Off –PoE Power Off. • Solid Amber –Port PoE overload or failure.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link. • Solid Green –Port links up at 25G. • Flashing –Transmit/Receive is activity.

QSFP+ 40G port LED

Feature	Detailed Description
QSFP+ 40G port LED	• Off – No Link. • Solid Green –Port links up at 40G. • Flashing –Transmit/Receive is activity.

S5860-48XMG Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	1. Temperature exceeds alarm threshold. 2. Power mixing.
	Solid red	1. System Failure. A. Board voltage abnormalities. B. Other hardware and software abnormalities, such as a chip cannot be initialized. 2. The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
FAN LED	Solid green	System FAN operating normally.
	Solid red	1. Any fan has failed: A. Model does not match system. B. The actual speed read is less than 3000 rpm (judged as stalled). C. Fan power_ok abnormality. 2. Any fan is not in position (see CPLD register);
PWR LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	A. Power module failure, no output of 12V, 54V. B. Power module not connected to AC power cord. C. Cannot read the model number of the power supply module. D. Can read the model number, but does not match the system.
MGMT LED	OFF	No Link.
	Solid green	Port linked operating at 1000M.
	Solid amber	Port linked operating at 10M or 100M.
	Flashing	Transmit/Receive is activity.

Port LED Definition

RJ45 100M/1G/2.5G/5G/10G port LED

Feature	Detailed Description
RJ45 100M/1G/2.5G/5G/10G port LED	• Off – No Link.

	• Solid Green –Port links up at 1G/2.5G/5G/10G. • Solid Amber –Port links up at 100M. • Flashing –Transmit/Receive is activity.

SFP28 25G port LED

Feature	Detailed Description
SFP28 25G port LED	• Off – No Link. • Solid Green –Port links up at 25G. • Flashing –Transmit/Receive is activity.

QSFP+ 40G port LED

Feature	Detailed Description
QSFP+ 40G port LED	• Off – No Link. • Solid Green –Port links up at 40G. • Flashing –Transmit/Receive is activity.

S5870-48T6S/S5870-48T6S-U Switch

System LED Definition

LED	Condition	Status
System Status LED (Bi-color LED)	• Solid Green – all functions are normal • Flashing Green –System diagnostic & OS in progress • Solid Amber –System diagnostic & OS Failed	At front
PSU1/PSU2 LED (Bi-color LED)	• Green – Normal • Amber –PSU1/PSU2 present but PG fail • Off – No main power supply present	At front
FAN Status LED (Bi-color LED)	• Green –Fan is OK • Amber – Fan tray fault • Off – The sku doesn't have system fan	At front
Location LED	Not supported.	At front
PoE LED (Only for AS4625-54P)	• Green – PoE loading << power budget • Amber –PoE loading ~ power budget • Off – None PoE sku	At front

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
1~48 Port	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP+ port status LED Indications

LED	Condition	Status
(Link/Activity) 49~54 Ports	Green Solid	Port Link on 10G mode
	Green Blinking	Port Link/Activity on 10G mode
	Amber Solid	Port Link on 1G mode

	Amber Blinking	Port Link/Activity on 1G mode

OOB Ethernet Port LEDs:

LED	Description
Link LED	• Solid green –The port is Link Up • Off –The port is Link Down
Activity LED	• Off – The port is no activity • Flashing Green – Activity

S5870-48T6BC/S5870-48T6BC-U Switch

System LED Definition

LED	Condition	Status
System LED	Green solid	System Diagnostic & OS OK
	Green Blinking	System Diagnostic & OS in progress
	Amber solid	System Diagnostic & OS Failed
PSU1 LED	Green solid	Power supply 1 operates normally
	Amber solid	Power supply 1 present but fault
	Off	Power supply 1 isn't presented. No PSU1
PSU2 LED	Green solid	Power supply 2 operates normally
	Amber solid	Power supply 2 present but fault
	Off	Power supply 2 isn't presented. No PSU2
FAN LED	Green solid	Fan works normally
	Amber solid	Fan fail
	Off	The SKU doesn't have system fan.
PoE LED	Green solid	PoE loading << power budget
	Amber solid	PoE loading ~ power budget
	Off	None PoE sku.
STK1/STK2 LED	Not in use.	
PRI LED	Not in use.	

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
0~47 Port (1~48)	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 49~52 Ports	Green solid	Port Link on 25G mode
	Green Blinking	Port Link/Activity on 25G mode
	White solid	Port Link on 10G mode
	White Blinking	Port Link/Activity on 10G mode
	Off	Link down

QSFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 53~54 Ports	White solid	Port Link on 100G mode
	White Blinking	Port Link/Activity on 100G mode
	Green solid	Port Link on 40G mode
	Green Blinking	Port Link/Activity on 40G mode
	Off	Link down

N5850-48X6C Switch

System LED Definition

Label	Condition	Description
PS1 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
PS2 (Power Supply Status)	Green	This power is operating normally.
	Amber	PWR present but not power on or this power is fault.
	Off	Power supply not present.
Diag	Green	System self-diagnostic test successfully completed.
	Amber	System self-diagnostic test has detected a fault. (Fan, thermal or any interface fault.)
FAN	Green	System FAN operating normally.
	Amber	Fan tray present buy system FAN is fault.
	OFF	System OFF
LOC	Not supported.	

Port LED Definition

LED	Condition	Status
1~48 Port LED	On/Flashing Green	RJ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Amber	RJ port has a valid link at 1G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 100G Mode (Port 49~ 54)	On/Flashing Green	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 25G Mode (With Breakout cable)	On/Flashing Amber	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.

QSFP28 Port LED in 40G Mode (Port 49~ 54)	On/Flashing blue	QSFP port has a valid link at 100G. Flashing indicates activity.
	Off	There is no link on the port.
QSFP28 Port LED in 10G Mode (With Breakout cable)	On/Flashing purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity.
	Off	There is no link on the port.
OOB LED (Link)	On	Port has a valid link
	Flashing	Flashing indicates activity
	Off	There is no link on the port

- Single-color LED will be used for 40/100G QSFP28 uplink port to indicate link/activity.
- There should be four LEDs per QSFP28 port. These LEDs can represent state of 40/100GE port or 4 10/25GE ports when used in breakout mode.
- The 40/100G QSFP28 LED should present OFF while there’s breakout cable plugged in.

N8550-64C Switch

System LED Definition

Feature	Detailed Description	Comment
Power Supply 1	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
Power Supply 2	• Red –Error/Failure/Bad • Green –Good • Off –Not present	At front
FANs	• Red –Error/Failure/Bad • Green –Good	At front
Diag	• Red –Error/Failure/Bad • Green –Good • Blinking Green –System boot in progress	At front
LOC	Not supported.	At front

Port LED Definition

Feature	Detailed Description
LED 1	• Blue – Link at 100Gbps (4 x 25G) • Orange– Link at 40Gbps (4 x 10G) • White– 25G • Green– 10G • OFF –not present
LED 2~4	• White– 25G • Green– 10G • OFF –not present

Management Port LED:

Feature	Detailed Description
LED	• Off –not present • Green – Link at 10/ 100M /1000M • Toggle – Activity

Console port LED:

Feature	Detailed Description
LED	• Off – No Link • Solid green – Link is present

N9550-32D Switch

System LED Definition

Feature	Detailed Description	Comment
Diagnosis LED	• Solid green – All OK, CLI prompt available • Blinking green – Boot-up in progress • Solid amber –System self-diagnostic test has detected a fault (Fan, thermal or any interface fault.).	At front
FAN LED	• Solid green –System FAN operating normally. • Solid amber –Fan tray present buy system FAN is fault. • OFF – System OFF.	At front
PS1 LED	• Solid green –This power is operating normally. • Solid amber –PWR present but not power on or this power is fault. • OFF – Power supply not present.	At rear
PS2 LED	• Solid green –This power is operating normally. • Solid amber –PWR present but not power on or this power is fault. • OFF – Power supply not present.	At front
Locator LED	Not supported.	At front

Port LED Definition

QSFP56-DD ports LED Indications

Only the 1st LED is used when running at 400G without breakout.
Solid Blue - Port linked operating at max port speed 400G.
Off - No link
Flashing Blue - Transmit/Receive is activity.
Only the 1st LED is used when running at 100G without breakout.
Solid Green - Port linked operating at max port speed 100G.
Off - No link
Flashing Green - Transmit/Receive is activity.
All four LEDs are used when running at 4 x 100G in breakout mode.
Solid Green - Port linked operating at max port speed 100G
Off - No link
Flashing Green -Transmit/Receive is activity
Three LEDs are used when running at 2 x 200G in breakout mode.

Solid blue (one LED), solid green (two LEDs) - Port linked operating at max port speed 200G
Off - No link
Flashing Green -Transmit/Receive is activity

Management Port LED SFP+

Feature	Detailed Description
SFP+ 10G management port LED	• Off – No Link • On/Flashing Green –SFP+ port has a valid link at 10G. Flashing indicates activity. • On/Flashing Amber –SFP+ port has a valid link at 1G. Flashing indicates activity.
RJ45 10/100/1G Management port LED	• Off – No Link • On/Flashing Green –Has a valid link. Flashing indicates activity.

S5870-48MX6BC-U Switch

System LED Definition

LED	Condition	Status
System LED	Green solid	System Diagnostic & OS OK.
	Green Blinking	System Diagnostic & OS in progress.
	Amber solid	System Diagnostic & OS Failed.
PSU1 LED	Green solid	Power supply 1 operates normally.
	Amber solid	Power supply 1 present but fault.
	Off	Power supply 1 isn’t presented. No PSU1.
PSU2 LED	Green solid	Power supply 2 operates normally.
	Amber solid	Power supply 2 present but fault.
	Off	Power supply 2 isn’t presented. No PSU2.
FAN LED	Green solid	Fan works normally.
	Amber solid	Fan fails.
	Off	The SKU doesn’t have system fan.
PoE LED	Green solid	PoE loading << power budget.
	Amber solid	PoE loading ~ power budget.
	Off	None PoE sku.
STK1/STK2 LED	Not in use.	
PRI LED	Not in use.	

Port LED Definition

RJ45 port status LED Indications

LED	Condition	Status
1~48 Port	Green solid	Port Link without POE
	Green Blinking	Port Link/Activity without POE
	Amber solid	Port Link with POE
	Amber Blinking	Port Link/Activity with POE

SFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 49~52 Ports	White solid	Port Link on 25G mode
	White Blinking	Port Link/Activity on 25G mode
	Green solid	Port Link on 10G mode
	Green Blinking	Port Link/Activity on 10G mode

QSFP28 port status LED Indications

LED	Condition	Status
(Link/Activity) 53~54 Ports	White solid	Port Link on 100G mode
	White Blinking	Port Link/Activity on 100G mode
	Green solid	Port Link on 40G mode
	Green Blinking	Port Link/Activity on 40G mode

S3410-24TS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	System (including any module) Failure.
PWR1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PWR2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
ID LED	Not in use.	

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – No Link. • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link. • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S3410L-24TF Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	System (including any module) Failure.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – No Link. • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

S3410L-24TF-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	System (including any module) Failure
LED Mode LED (controlled by LED Mode button on the front panel)	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by LED Mode button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

S3410-24TS-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold 50ºC but less than 60ºC.
	Solid red	System (including any module) Failure
PWR1 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
PWR2 LED	OFF	Power supply not present.
	Solid green	This power is operating normally.
	Solid red	Power module failure or need to connect to the AC power line.
M1/M2 LED	Not in use.	
PoE LED (controlled by PoE button on the front panel)	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP 1G port LED (23, 24)

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link. • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S3410C-8TMS-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold.
	Solid red	• System Failure. • The temperature of any part of the switch exceeds the maximum temperature allowed by the device.
PoE LED (controlled by Mode button on the front panel)	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by Mode button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1000M, 100M or 10M. • Flashing –Transmit/Receive is activity.
PoE (controlled by Mode button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description

SFP+ 10G port LED	• Off – No Link. • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

S3410C-16TF Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold.
	Solid red	• System Failure. • The temperature of any part of the machine exceeds the maximum temperature allowed by the device.

Port LED Definition

110/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – No Link. • Solid Green –Port links up at 10M, 100M or 100M. • Flashing –Transmit/Receive is activity.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

S3410C-16TMS-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold.
	Solid red	• System Failure. • The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
POE LED	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 10M, 100M or 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

1000M/2.5G/5GBASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1000M,2.5G or 5G. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP+ 1/10G port LED

Feature	Detailed Description
SFP+ 1/10G port LED	• Off – No Link. • Solid Green –Port links up at 1G or 10G. • Flashing –Transmit/Receive is activity.

S3410C-16TF-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid green	The system completes initialization and works normally.
	Solid amber	Temperature exceeds alarm threshold.
	Solid red	• System Failure. • The temperature of any part of the machine exceeds the maximum temperature allowed by the device.
POE LED	Solid green	Port LEDs indicate data switching status.
	Solid amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 10M,100M or 1000M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

S3410-48TS-P Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking Green	Boot-up in progress.
	Solid Green	The system completes initialization and works normally.
	Solid Amber	Temperature exceeds alarm threshold.
	Solid Red	• System Failure. • The temperature of any part of the switch exceeds the maximum temperature allowed by the device.
PWR1 LED	OFF	Power supply not present.
	Solid Green	This power is operating normally.
	Solid Red	Power module failure or need to connect to AC power line.
PWR2 LED	OFF	Power supply not present.
	Solid Green	This power is operating normally.
	Solid Red	Power module failure or need to connect to AC power line.
M1/M2 LED	Not supported.	
PoE LED (controlled by PoE button on the front panel)	Solid Green	Port LEDs indicate data switching status.
	Solid Amber	Port LEDs indicate PoE power supply status.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
Non-PoE (controlled by PoE button on the front panel)	• Off – No Link. • Solid Green –Port links up at 1000M. • Solid Amber –Port links up at 10M or 100M. • Flashing –Transmit/Receive is activity.
PoE (controlled by PoE button on the front panel)	• Solid Green –PoE Power On. • Solid Amber – PoE Overload. • Solid Red –PoE Failure. • Off –PoE Power Off.

SFP 1G port LED (47, 48)

Feature	Detailed Description
SFP 1G port LED	• Off – No Link. • Solid Green –Port links up at 1G. • Flashing –Transmit/Receive is activity.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – No Link. • Solid Green –Port links up at 10G or 1G. • Flashing –Transmit/Receive is activity.

N8550-48B8C Switch

System LED Definition

LED	Color	Mode
Power Supply 1	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
Power Supply 2	Red	Error/Failure/Bad
	Green	Good
	Off	Not present
FANs	Red	Error/Failure/Bad
	Green	Good
Diag	Red	Error/Fault/Failure
	Green	Good
	Blinking Green	System boot in progress
LOC	Not supported.	

Port LED Definition

SFP28 Port LED Definition

LED	Color	Mode
SFP28 Port LED	On/Flashing Green	SFP28 port has a valid link at 25G. Flashing indicates activity.
	On/Flashing Yellow	SFP28 port has a valid link at 10G. Flashing indicates activity.
	OFF	There is no link on the port.

QSFP28 Port LED Definition

LED	Color	Mode
LED 1~4 (Port 49~56)	On/Flashing Green	QSFP28 port has a valid link at 100G. Flashing indicates activity.
	OFF	There is no link on the port.

	On/Flashing Blue	QSFP28 port has a valid link at 40G. Flashing indicates activity.
	OFF	There is no link on the port.
	On/Flashing Yellow	QSFP28 port has a valid link at 25G via break out cable. The LED on 100G QSFP end is also present OFF. Flashing indicates activity. (With Breakout cable)
	OFF	There is no link on the port.
	On/Flashing Purple	QSFP28 port has a valid link at 10G via break out cable. The LED on 40G QSFP end is also present OFF. Flashing indicates activity. (With Breakout cable)
	OFF	There is no link on the port

SFP+ Port LED Definition

LED	Color	Mode
SFP+ Port LED	On/Flashing Green	SFP+ port has a valid link at 10G. Flashing indicates activity.
	On/Flashing Yellow	SFP+ port has a valid link at 1G. Flashing indicates activity.
	OFF	There is no link on the port.

Management Port LED

LED	Color	Mode
MGMT Port LED	On Green	Port has a valid link
	Flashing Yellow	Flashing indicates activity
	OFF	There is no link on the port.

S3410-48TS Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid Green	The switch is operational.
	Solid Amber	Moderate temperature warning: Check the working environment of the switch immediately.
	Solid Red	• Severe temperature warning: The temperature severely exceeds the temperature limit, so the system is going to restart. • The switch is faulty.
PWR1/PWR2 LED	Off	No power supply module is connected.
	Solid Green	A power supply is connected and enable to work.
	Solid Red	Redundant power fails or no AC cable is connected.
ID LED	Off	Locating is disabled.
	Solid Bule	Locating is enabled. Operation and maintenance staff turn on and off the LED remotely.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – The port is not connected.. • Solid Green – The port is connected at 1000M. • Solid Amber – The port is connected at 10M/ 100M. • Flashing – Data is being received or transmitted.

SFP+ 10G port LED

Feature	Detailed Description
SFP+ 10G port LED	• Off – The port is not connected. • Solid Green – The port is connected. • Flashing – The port is receiving or transmitted traffic.

S3410L-48TF Switch

System LED Definition

LED Name	Status	Detailed Description
Status LED	OFF	No power supply.
	Blinking green	Boot-up in progress.
	Solid Green	The switch is operational.
	Solid Amber	Moderate temperature warning: Check the working environment of the switch immediately.
	Solid Red	• Severe temperature warning: The temperature severely exceeds the temperature limit, so the system is going to restart. • The switch is faulty.
PSU LED	Off	No power supply module is connected.
	Solid Green	A power supply is connected and enable to work.
	Solid Red	Redundant power fails or no AC cable is connected.
ID LED	Off	Locating is disabled.
	Solid Bule	Locating is enabled. Operation and maintenance staff turn on and off the LED remotely.

Port LED Definition

10/100/1000BASE-T RJ45 port LED

Feature	Detailed Description
10/100/1000BASE-T RJ45 port LED	• Off – The port is not connected.. • Solid Green – The port is connected at 1000M. • Solid Amber – The port is connected at 10M/ 100M. • Flashing – Data is being received or transmitted.

SFP 1G port LED

Feature	Detailed Description
SFP 1G port LED	• Off – The port is not connected. • Solid Green – The port is connected. • Flashing – The port is receiving or transmitted traffic.

N8550-24CD8D Switch

System LED Definition

LED Name	Status	Detailed Description
SYS LED	Off	No power supply.
	Blinking Green	The system is initializing.
	Solid Red	The system is working abnormally.
	Solid Green	The system completes initialization and works normally.
PSU LED (Front Panel)	OFF	No power supply inserted.
	Solid Red	There is a PSU working abnormally.
	Solid Green	All power supplies are operating normally.
PSU LED (Rear Panel)	IN	Power input normal.
	OUT	Power supply is normal.
	!	Power is operating abnormally.
FAN LED (Front Panel)	OFF	No fan inserted.
	Solid Green	All fans operate normally.
	Solid Red	There is fan is working abnormally.
FAN LED (Rear Panel)	OFF	No fan inserted.
	Solid Green	The fan operates normally.
	Solid Red	The fan is working abnormally.
MGMT LED	OFF	No Link.
	Solid Green	Port linked operating at 10M, 100M or 1000M.
	Flashing Amber/Green	Transmit/Receive is activity, Port linked operating at 10000M.
ID LED	Not supported.	

Port LED Definition

200GB QSFP56 port LED

LED Name	Status	Detailed Description
24 x 200GB QSFP56 port LED	Off	The port is not connected.
	Solid Green	Port linked operating at max port speed.
	Solid Amber	The system is launching **lcmgr** process.
	Blinking Green	Data is being received or transmitted.

400GB QSFP-DD port LED

LED Name	Status	Detailed Description
8 x 400GB QSFP56 port LED	Off	The port is not connected.
	Solid Green	Port linked operating at max port speed.
	Solid Amber	The system is launching **lcmgr** process.
	Blinking Green	Data is being received or transmitted.

N9600-64OD Switch

System LED Definition

LED Name	Status	Detailed Description
SYS LED	OFF	No power supply.
	Solid green	The system completes initialization and works normally.
	Blinking amber	The system is initializing.
LINK/ACT LED	OFF	The port is not connected.
	Solid green	Port links up at 1G/100M/10M.
	Blinking green	Data is being received or transmitted.
PSU LED (front panel)	OFF	No power supply inserted.
	Blinking amber	Not all power supplies are operating normally.
	Solid green	Two power supplies are operating normally.
FAN LED (front panel)	OFF	No fan inserted.
	Solid amber	Not all fans are operating normally.
	Solid green	Four fans are operating normally.
BMC LED	Not supported.	
25G SFP28 port LED	Not supported.	
PSU LED (rear panel)	Solid green (IN)	Power input normal.
	Solid green (OUT)	Power supply is normal.
	Solid amber (!)	The PSU module is not powered on or is not operating abnormally.
FAN LED (rear panel)	OFF	No fan inserted.
	Solid green	The fan is operating normally.
800GB OSFP port LED	Off	The port links down.
	Solid Green	Port links up at 800G, split speed of 400G/200G/100G, and reduced speed of 400G/200G/100G/50G.
	Blinking Green	Data is being received or transmitted.

Port Index Description

- Dell Switch Port Name Description
  - N2224X-ON/N2224PX-ON Switch Port Name Description
  - N2248X-ON/N2248PX-ON Switch Port Name Description
  - N3208PX-ON Switch Port Name Description
  - N3224F-ON/N3224T-ON Switch Port Name Description
  - N3224P-ON Switch Port Name Description
  - N3224PX-ON Switch Port Name Description
  - N3248P-ON/N3248TE-ON Switch Port Name Description
  - N3248PXE-ON/N3248X-ON Switch Port Name Description
  - S4048-ON Switch Port Name Description
  - S4148T-ON Switch Port Name Description
  - S5212F-ON Switch Port Name Description
  - S5224F-ON Switch Port Name Description
  - S5232F-ON Switch Port Name Description
  - S5248F Switch Port Name Description
  - S5296F-ON Switch Port Name Description
  - Z9100-ON Switch Port Name Description
  - Z9264F-ON Switch Port Name Description
  - S4128F-ON Switch Port Name Description
  - S4128T-ON Switch Port Name Description
  - S4148F-ON Switch Port Name Description
- EdgeCore/Accton Switch Port Name Description
  - AS5812_54T/AS5812_54X Switch Port Name Description
  - AS4625-54P/AS4625-54T Switch Port Name Description
  - AS4630-54NPE Switch Port Name Description
  - AS4630-54PE Switch Port Name Description
  - AS6812_32X Switch Port Name Description
  - AS7312-54X/AS7312_54XS Switch Port Name Description
  - AS7326-56X Switch Port Name Description
  - AS7726-32X Switch Port Name Description
  - AS7816-64X Switch Port Name Description
  - AS9716-32D Switch Port Name Description
  - AS4610_30T/AS4610_30P Switch Port Name Description
  - AS4610_54T/AS4610_54P Switch Port Name Description
  - AS5712_54X Switch Port Name Description
  - AS5835_54X/AS5835_54T Switch Port Name Description
  - AS7712_32X Switch Port Name Description
- Delta/Agema Switch Port Name Description
  - AG5648V1 Switch Port Name Description
  - AG7648 Switch Port Name Description
  - AG9032v1 Switch Port Name Description
- FS Switch Port Name Description
  - N5850-48S6Q Switch Port Name Description
  - N8550-32C Switch Port Name Description
  - N8550-48B8C Switch Port Name Description
  - S5810-48TS-P Switch Port Name Description
  - S5810-28FS Switch Port Name Description
  - S5810-28TS Switch Port Name Description
  - S5810-48FS Switch Port Name Description
  - S5810-48TS Switch Port Name Description
  - S5860-20SQ Switch Port Name Description
  - S5860-24XB-U Switch Port Name Description
  - N8560-32C Switch Port Name Description
  - N8560-64C Switch Port Name Description
  - S5860-24MG-U Switch Port Name Description
  - S5860-48XMG-U/S5860-48XMG Switch Port Name Description
  - S5860-24XMG Switch Port Name Description
  - S5860-48MG-U Switch Port Name Description
  - S5870-48T6S-U/S5870-48T6S Switch Port Name Description
  - S5870-48T6BC/S5870-48T6BC-U Switch Port Name Description
  - N5850-48X6C Switch Port Name Description
  - N8550-64C Switch Port Name Description
  - N9550-32D Switch Port Name Description
  - N5850-48S6C Switch Port Name Description
  - S5870-48MX6BC-U Switch Port Name Description

- S3410-24TS Switch Port Name Description
- S3410L-24TF Switch Port Name Description
- S3410L-24TF-P Switch Port Name Description
- S3410-24TS-P Switch Port Name Description
- S3410C-16TMS-P Switch Port Name Description
- S3410C-16TF-P Switch Port Name Description
- S3410C-8TMS-P Switch Port Name Description
- S3410C-16TF Switch Port Name Description
- S3410-48TS-P Switch Port Name Description
- S3410-48TS Switch Port Name Description
- S3410L-48TF Switch Port Name Description
- N8550-24CD8D Switch Port Name Description
- N9600-64OD Switch Port Name Description

Note
If user plugs in a DAC line on OVS mode, user should enable it. The configuration refers to: OVS Configuration Guide/Configuring Open vSwitch/Creating a Bridge/Adding Ports to a Bridge

Dell Switch Port Name Description

- N2224X-ON/N2224PX-ON Switch Port Name Description
- N2248X-ON/N2248PX-ON Switch Port Name Description
- N3208PX-ON Switch Port Name Description
- N3224F-ON/N3224T-ON Switch Port Name Description
- N3224P-ON Switch Port Name Description
- N3224PX-ON Switch Port Name Description
- N3248P-ON/N3248TE-ON Switch Port Name Description
- N3248PXE-ON/N3248X-ON Switch Port Name Description
- S4048-ON Switch Port Name Description
- S4148T-ON Switch Port Name Description
- S5212F-ON Switch Port Name Description
- S5224F-ON Switch Port Name Description
- S5232F-ON Switch Port Name Description
- S5248F Switch Port Name Description
- S5296F-ON Switch Port Name Description
- Z9100-ON Switch Port Name Description
- Z9264F-ON Switch Port Name Description
- S4128F-ON Switch Port Name Description
- S4128T-ON Switch Port Name Description
- S4148F-ON Switch Port Name Description

N2224X-ON/N2224PX-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	2.5Gb/s, 1Gb/s, 100Mb/s
2	ge-1/1/2	2.5Gb/s, 1Gb/s, 100Mb/s
3	ge-1/1/3	2.5Gb/s, 1Gb/s, 100Mb/s
4	ge-1/1/4	2.5Gb/s, 1Gb/s, 100Mb/s
5	ge-1/1/5	2.5Gb/s, 1Gb/s, 100Mb/s
6	ge-1/1/6	2.5Gb/s, 1Gb/s, 100Mb/s
7	ge-1/1/7	2.5Gb/s, 1Gb/s, 100Mb/s
8	ge-1/1/8	2.5Gb/s, 1Gb/s, 100Mb/s
9	ge-1/1/9	2.5Gb/s, 1Gb/s, 100Mb/s
10	ge-1/1/10	2.5Gb/s, 1Gb/s, 100Mb/s
11	ge-1/1/11	2.5Gb/s, 1Gb/s, 100Mb/s
12	ge-1/1/12	2.5Gb/s, 1Gb/s, 100Mb/s
13	ge-1/1/13	2.5Gb/s, 1Gb/s, 100Mb/s
14	ge-1/1/14	2.5Gb/s, 1Gb/s, 100Mb/s
15	ge-1/1/15	2.5Gb/s, 1Gb/s, 100Mb/s
16	ge-1/1/16	2.5Gb/s, 1Gb/s, 100Mb/s
17	ge-1/1/17	2.5Gb/s, 1Gb/s, 100Mb/s
18	ge-1/1/18	2.5Gb/s, 1Gb/s, 100Mb/s
19	ge-1/1/19	2.5Gb/s, 1Gb/s, 100Mb/s
20	ge-1/1/20	2.5Gb/s, 1Gb/s, 100Mb/s
21	ge-1/1/21	2.5Gb/s, 1Gb/s, 100Mb/s
22	ge-1/1/22	2.5Gb/s, 1Gb/s, 100Mb/s
23	ge-1/1/23	2.5Gb/s, 1Gb/s, 100Mb/s
24	ge-1/1/24	2.5Gb/s, 1Gb/s, 100Mb/s
25	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
29	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
30	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s

N2248X-ON/N2248PX-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	2.5Gb/s, 1Gb/s, 100Mb/s
2	ge-1/1/2	2.5Gb/s, 1Gb/s, 100Mb/s
3	ge-1/1/3	2.5Gb/s, 1Gb/s, 100Mb/s
4	ge-1/1/4	2.5Gb/s, 1Gb/s, 100Mb/s
5	ge-1/1/5	2.5Gb/s, 1Gb/s, 100Mb/s
6	ge-1/1/6	2.5Gb/s, 1Gb/s, 100Mb/s
7	ge-1/1/7	2.5Gb/s, 1Gb/s, 100Mb/s
8	ge-1/1/8	2.5Gb/s, 1Gb/s, 100Mb/s
9	ge-1/1/9	2.5Gb/s, 1Gb/s, 100Mb/s
10	ge-1/1/10	2.5Gb/s, 1Gb/s, 100Mb/s
11	ge-1/1/11	2.5Gb/s, 1Gb/s, 100Mb/s
12	ge-1/1/12	2.5Gb/s, 1Gb/s, 100Mb/s
13	ge-1/1/13	2.5Gb/s, 1Gb/s, 100Mb/s
14	ge-1/1/14	2.5Gb/s, 1Gb/s, 100Mb/s
15	ge-1/1/15	2.5Gb/s, 1Gb/s, 100Mb/s
16	ge-1/1/16	2.5Gb/s, 1Gb/s, 100Mb/s
17	ge-1/1/17	2.5Gb/s, 1Gb/s, 100Mb/s
18	ge-1/1/18	2.5Gb/s, 1Gb/s, 100Mb/s
19	ge-1/1/19	2.5Gb/s, 1Gb/s, 100Mb/s
20	ge-1/1/20	2.5Gb/s, 1Gb/s, 100Mb/s
21	ge-1/1/21	2.5Gb/s, 1Gb/s, 100Mb/s
22	ge-1/1/22	2.5Gb/s, 1Gb/s, 100Mb/s
23	ge-1/1/23	2.5Gb/s, 1Gb/s, 100Mb/s
24	ge-1/1/24	2.5Gb/s, 1Gb/s, 100Mb/s
25	ge-1/1/25	2.5Gb/s, 1Gb/s, 100Mb/s
26	ge-1/1/26	2.5Gb/s, 1Gb/s, 100Mb/s
27	ge-1/1/27	2.5Gb/s, 1Gb/s, 100Mb/s
28	ge-1/1/28	2.5Gb/s, 1Gb/s, 100Mb/s
29	ge-1/1/29	2.5Gb/s, 1Gb/s, 100Mb/s
30	ge-1/1/30	2.5Gb/s, 1Gb/s, 100Mb/s
31	ge-1/1/31	2.5Gb/s, 1Gb/s, 100Mb/s
32	ge-1/1/32	2.5Gb/s, 1Gb/s, 100Mb/s
33	ge-1/1/33	2.5Gb/s, 1Gb/s, 100Mb/s
34	ge-1/1/34	2.5Gb/s, 1Gb/s, 100Mb/s
35	ge-1/1/35	2.5Gb/s, 1Gb/s, 100Mb/s
36	ge-1/1/36	2.5Gb/s, 1Gb/s, 100Mb/s
37	ge-1/1/37	2.5Gb/s, 1Gb/s, 100Mb/s
38	ge-1/1/38	2.5Gb/s, 1Gb/s, 100Mb/s
39	ge-1/1/39	2.5Gb/s, 1Gb/s, 100Mb/s

Physical Port Number	Interface Names	Interface Supported Speed
40	ge-1/1/40	2.5Gb/s, 1Gb/s, 100Mb/s
41	ge-1/1/41	2.5Gb/s, 1Gb/s, 100Mb/s
42	ge-1/1/42	2.5Gb/s, 1Gb/s, 100Mb/s
43	ge-1/1/43	2.5Gb/s, 1Gb/s, 100Mb/s
44	ge-1/1/44	2.5Gb/s, 1Gb/s, 100Mb/s
45	ge-1/1/45	2.5Gb/s, 1Gb/s, 100Mb/s
46	ge-1/1/46	2.5Gb/s, 1Gb/s, 100Mb/s
47	ge-1/1/47	2.5Gb/s, 1Gb/s, 100Mb/s
48	ge-1/1/48	2.5Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/49	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/50	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/51	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/52	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s

N3208PX-ON Switch Port Name Description

Mapping between physical ports, interface names and interface supported speeds are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	1Gb/s, 100Mb/s, 10Mb/s
2	ge-1/1/2	1Gb/s, 100Mb/s, 10Mb/s
3	ge-1/1/3	1Gb/s, 100Mb/s, 10Mb/s
4	ge-1/1/4	1Gb/s, 100Mb/s, 10Mb/s
5	ge-1/1/5	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s, 10Mb/s
6	ge-1/1/6	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s, 10Mb/s
7	ge-1/1/7	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s, 10Mb/s
8	ge-1/1/8	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s, 10Mb/s
9	te-1/1/1	10Gb/s, 1Gb/s
10	te-1/1/2	10Gb/s, 1Gb/s

N3224F-ON/N3224T-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	te-1/1/1	1Gb/s
2	te-1/1/2	1Gb/s
3	te-1/1/3	1Gb/s
4	te-1/1/4	1Gb/s
5	te-1/1/5	1Gb/s
6	te-1/1/6	1Gb/s
7	te-1/1/7	1Gb/s
8	te-1/1/8	1Gb/s
9	te-1/1/9	1Gb/s
10	te-1/1/10	1Gb/s
11	te-1/1/11	1Gb/s
12	te-1/1/12	1Gb/s
13	te-1/1/13	1Gb/s
14	te-1/1/14	1Gb/s
15	te-1/1/15	1Gb/s
16	te-1/1/16	1Gb/s
17	te-1/1/17	1Gb/s
18	te-1/1/18	1Gb/s
19	te-1/1/19	1Gb/s
20	te-1/1/20	1Gb/s
21	te-1/1/21	1Gb/s
22	te-1/1/22	1Gb/s
23	te-1/1/23	1Gb/s
24	te-1/1/24	1Gb/s
25	te-1/1/25	10Gb/s,1Gb/s
26	te-1/1/26	10Gb/s,1Gb/s
27	te-1/1/27	10Gb/s,1Gb/s
28	te-1/1/28	10Gb/s,1Gb/s
29	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

N3224P-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	te-1/1/1	1Gb/s, 100Mb/s, 10Mb/s
2	te-1/1/2	1Gb/s, 100Mb/s, 10Mb/s
3	te-1/1/3	1Gb/s, 100Mb/s, 10Mb/s
4	te-1/1/4	1Gb/s, 100Mb/s, 10Mb/s
5	te-1/1/5	1Gb/s, 100Mb/s, 10Mb/s
6	te-1/1/6	1Gb/s, 100Mb/s, 10Mb/s
7	te-1/1/7	1Gb/s, 100Mb/s, 10Mb/s
8	te-1/1/8	1Gb/s, 100Mb/s, 10Mb/s
9	te-1/1/9	1Gb/s, 100Mb/s, 10Mb/s
10	te-1/1/10	1Gb/s, 100Mb/s, 10Mb/s
11	te-1/1/11	1Gb/s, 100Mb/s, 10Mb/s
12	te-1/1/12	1Gb/s, 100Mb/s, 10Mb/s
13	te-1/1/13	1Gb/s, 100Mb/s, 10Mb/s
14	te-1/1/14	1Gb/s, 100Mb/s, 10Mb/s
15	te-1/1/15	1Gb/s, 100Mb/s, 10Mb/s
16	te-1/1/16	1Gb/s, 100Mb/s, 10Mb/s
17	te-1/1/17	1Gb/s, 100Mb/s, 10Mb/s
18	te-1/1/18	1Gb/s, 100Mb/s, 10Mb/s
19	te-1/1/19	1Gb/s, 100Mb/s, 10Mb/s
20	te-1/1/20	1Gb/s, 100Mb/s, 10Mb/s
21	te-1/1/21	1Gb/s, 100Mb/s, 10Mb/s
22	te-1/1/22	1Gb/s, 100Mb/s, 10Mb/s
23	te-1/1/23	1Gb/s, 100Mb/s, 10Mb/s
24	te-1/1/24	1Gb/s, 100Mb/s, 10Mb/s
25	te-1/1/25	10Gb/s,1Gb/s
26	te-1/1/26	10Gb/s,1Gb/s
27	te-1/1/27	10Gb/s,1Gb/s
28	te-1/1/28	10Gb/s,1Gb/s
29	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

N3224PX-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	te-1/1/1	10/100/1000Mb/s or 2.5/5G/10Gb/s
2	te-1/1/2	10/100/1000Mb/s or 2.5/5G/10Gb/s
3	te-1/1/3	10/100/1000Mb/s or 2.5/5G/10Gb/s
4	te-1/1/4	10/100/1000Mb/s or 2.5/5G/10Gb/s
5	te-1/1/5	10/100/1000Mb/s or 2.5/5G/10Gb/s
6	te-1/1/6	10/100/1000Mb/s or 2.5/5G/10Gb/s
7	te-1/1/7	10/100/1000Mb/s or 2.5/5G/10Gb/s
8	te-1/1/8	10/100/1000Mb/s or 2.5/5G/10Gb/s
9	te-1/1/9	10/100/1000Mb/s or 2.5/5G/10Gb/s
10	te-1/1/10	10/100/1000Mb/s or 2.5/5G/10Gb/s
11	te-1/1/11	10/100/1000Mb/s or 2.5/5G/10Gb/s
12	te-1/1/12	10/100/1000Mb/s or 2.5/5G/10Gb/s
13	te-1/1/13	10/100/1000Mb/s or 2.5/5G/10Gb/s
14	te-1/1/14	10/100/1000Mb/s or 2.5/5G/10Gb/s
15	te-1/1/15	10/100/1000Mb/s or 2.5/5G/10Gb/s
16	te-1/1/16	10/100/1000Mb/s or 2.5/5G/10Gb/s
17	te-1/1/17	10/100/1000Mb/s or 2.5/5G/10Gb/s
18	te-1/1/18	10/100/1000Mb/s or 2.5/5G/10Gb/s
19	te-1/1/19	10/100/1000Mb/s or 2.5/5G/10Gb/s
20	te-1/1/20	10/100/1000Mb/s or 2.5/5G/10Gb/s
21	te-1/1/21	10/100/1000Mb/s or 2.5/5G/10Gb/s
22	te-1/1/22	10/100/1000Mb/s or 2.5/5G/10Gb/s
23	te-1/1/23	10/100/1000Mb/s or 2.5/5G/10Gb/s
24	te-1/1/24	10/100/1000Mb/s or 2.5/5G/10Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

N3248P-ON/N3248TE-ON Switch Port Name Description

Mapping between physical ports, interface names and interface supported speeds are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	1Gb/s, 100Mb/s, 10Mb/s
2	ge-1/1/2	1Gb/s, 100Mb/s, 10Mb/s
3	ge-1/1/3	1Gb/s, 100Mb/s, 10Mb/s
4	ge-1/1/4	1Gb/s, 100Mb/s, 10Mb/s
5	ge-1/1/5	1Gb/s, 100Mb/s, 10Mb/s
6	ge-1/1/6	1Gb/s, 100Mb/s, 10Mb/s
7	ge-1/1/7	1Gb/s, 100Mb/s, 10Mb/s
8	ge-1/1/8	1Gb/s, 100Mb/s, 10Mb/s
9	ge-1/1/9	1Gb/s, 100Mb/s, 10Mb/s
10	ge-1/1/10	1Gb/s, 100Mb/s, 10Mb/s
11	ge-1/1/11	1Gb/s, 100Mb/s, 10Mb/s
12	ge-1/1/12	1Gb/s, 100Mb/s, 10Mb/s
13	ge-1/1/13	1Gb/s, 100Mb/s, 10Mb/s
14	ge-1/1/14	1Gb/s, 100Mb/s, 10Mb/s
15	ge-1/1/15	1Gb/s, 100Mb/s, 10Mb/s
16	ge-1/1/16	1Gb/s, 100Mb/s, 10Mb/s
17	ge-1/1/17	1Gb/s, 100Mb/s, 10Mb/s
18	ge-1/1/18	1Gb/s, 100Mb/s, 10Mb/s
19	ge-1/1/19	1Gb/s, 100Mb/s, 10Mb/s
20	ge-1/1/20	1Gb/s, 100Mb/s, 10Mb/s
21	ge-1/1/21	1Gb/s, 100Mb/s, 10Mb/s
22	ge-1/1/22	1Gb/s, 100Mb/s, 10Mb/s
23	ge-1/1/23	1Gb/s, 100Mb/s, 10Mb/s
24	ge-1/1/24	1Gb/s, 100Mb/s, 10Mb/s
25	ge-1/1/25	1Gb/s, 100Mb/s, 10Mb/s
26	ge-1/1/26	1Gb/s, 100Mb/s, 10Mb/s
27	ge-1/1/27	1Gb/s, 100Mb/s, 10Mb/s
28	ge-1/1/28	1Gb/s, 100Mb/s, 10Mb/s
29	ge-1/1/29	1Gb/s, 100Mb/s, 10Mb/s
30	ge-1/1/30	1Gb/s, 100Mb/s, 10Mb/s
31	ge-1/1/31	1Gb/s, 100Mb/s, 10Mb/s
32	ge-1/1/32	1Gb/s, 100Mb/s, 10Mb/s
33	ge-1/1/33	1Gb/s, 100Mb/s, 10Mb/s
34	ge-1/1/34	1Gb/s, 100Mb/s, 10Mb/s
35	ge-1/1/35	1Gb/s, 100Mb/s, 10Mb/s
36	ge-1/1/36	1Gb/s, 100Mb/s, 10Mb/s
37	ge-1/1/37	1Gb/s, 100Mb/s, 10Mb/s
38	ge-1/1/38	1Gb/s, 100Mb/s, 10Mb/s
39	ge-1/1/39	1Gb/s, 100Mb/s, 10Mb/s

40	ge-1/1/40	1Gb/s, 100Mb/s, 10Mb/s
41	ge-1/1/41	1Gb/s, 100Mb/s, 10Mb/s
42	ge-1/1/42	1Gb/s, 100Mb/s, 10Mb/s
43	ge-1/1/43	1Gb/s, 100Mb/s, 10Mb/s
44	ge-1/1/44	1Gb/s, 100Mb/s, 10Mb/s
45	ge-1/1/45	1Gb/s, 100Mb/s, 10Mb/s
46	ge-1/1/46	1Gb/s, 100Mb/s, 10Mb/s
47	ge-1/1/47	1Gb/s, 100Mb/s, 10Mb/s
48	ge-1/1/48	1Gb/s, 100Mb/s, 10Mb/s
49	te-1/1/1	10Gb/s, 1Gb/s
50	te-1/1/2	10Gb/s, 1Gb/s
51	te-1/1/3	10Gb/s, 1Gb/s
52	te-1/1/4	10Gb/s, 1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

N3248PXE-ON/N3248X-ON Switch Port Name Description

NOTE:
Ports Te-1 / 1/49, Te-1 / 1/50, Te-1 / 1/51 and Te-1 / 1/52 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/49	te-1/1/50	te-1/1/51	te-1/1/52	Allowed or not Allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note: If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

Mapping between physical ports, interface names and interface supported speeds are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
2	te-1/1/2	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
3	te-1/1/3	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
4	te-1/1/4	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
5	te-1/1/5	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
6	te-1/1/6	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
7	te-1/1/7	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
8	te-1/1/8	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
9	te-1/1/9	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
10	te-1/1/10	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
11	te-1/1/11	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
12	te-1/1/12	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
13	te-1/1/13	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
14	te-1/1/14	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
15	te-1/1/15	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
16	te-1/1/16	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
17	te-1/1/17	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
18	te-1/1/18	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
19	te-1/1/19	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
20	te-1/1/20	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
21	te-1/1/21	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
22	te-1/1/22	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
23	te-1/1/23	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
24	te-1/1/24	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
25	te-1/1/25	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
26	te-1/1/26	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s

27	te-1/1/27	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
28	te-1/1/28	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
29	te-1/1/29	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
30	te-1/1/30	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
31	te-1/1/31	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
32	te-1/1/32	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
33	te-1/1/33	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
34	te-1/1/34	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
35	te-1/1/35	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
36	te-1/1/36	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
37	te-1/1/37	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
38	te-1/1/38	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
39	te-1/1/39	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
40	te-1/1/40	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
41	te-1/1/41	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
42	te-1/1/42	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
43	te-1/1/43	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
44	te-1/1/44	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
45	te-1/1/45	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
46	te-1/1/46	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
47	te-1/1/47	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
48	te-1/1/48	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/49	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/50	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/51	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/52	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

S4048-ON Switch Port Name Description

Mapping between physical port, interface names and interface support speed on S4048-ON are in the following table.

Physical Port Number	Interface Names	interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s
27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s

40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
50	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
51	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
52	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
53	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s

S4148T-ON Switch Port Name Description

NOTEs:
The uplink ports, with port numbers from 25 to 30, have two different uplink port modes 6x40G (default) and 4x100G.

- You need to change the port mode to 4x100G if you want to use 100G uplinks, please refer to following page with instructions to set up the port mode:

Configuring Port Mapping On S4148 Series Switch

- Ports with physical port number 27 & 28 are only available in the 6x40G mode and are not available in the 4x100G mode.

Mapping between physical ports, interface names and interface support speed of S4148T-ON are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s,1Gb/s, 100Mb/s
2	te-1/1/2	10Gb/s,1Gb/s, 100Mb/s
3	te-1/1/3	10Gb/s,1Gb/s, 100Mb/s
4	te-1/1/4	10Gb/s,1Gb/s, 100Mb/s
5	te-1/1/5	10Gb/s,1Gb/s, 100Mb/s
6	te-1/1/6	10Gb/s,1Gb/s, 100Mb/s
7	te-1/1/7	10Gb/s,1Gb/s, 100Mb/s
8	te-1/1/8	10Gb/s,1Gb/s, 100Mb/s
9	te-1/1/9	10Gb/s,1Gb/s, 100Mb/s
10	te-1/1/10	10Gb/s,1Gb/s, 100Mb/s
11	te-1/1/11	10Gb/s,1Gb/s, 100Mb/s
12	te-1/1/12	10Gb/s,1Gb/s, 100Mb/s
13	te-1/1/13	10Gb/s,1Gb/s, 100Mb/s
14	te-1/1/14	10Gb/s,1Gb/s, 100Mb/s
15	te-1/1/15	10Gb/s,1Gb/s, 100Mb/s
16	te-1/1/16	10Gb/s,1Gb/s, 100Mb/s
17	te-1/1/17	10Gb/s,1Gb/s, 100Mb/s
18	te-1/1/18	10Gb/s,1Gb/s, 100Mb/s
19	te-1/1/19	10Gb/s,1Gb/s, 100Mb/s
20	te-1/1/20	10Gb/s,1Gb/s, 100Mb/s
21	te-1/1/21	10Gb/s,1Gb/s, 100Mb/s
22	te-1/1/22	10Gb/s,1Gb/s, 100Mb/s
23	te-1/1/23	10Gb/s,1Gb/s, 100Mb/s
24	te-1/1/24	10Gb/s,1Gb/s, 100Mb/s
25	• **When port mode is 6x40G (default)** xe-1/1/1 • **When port mode is 4x100G** xe-1/1/1	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	• **When port mode is 6x40G (default)** xe-1/1/2 • **When port mode is 4x100G** xe-1/1/2	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	• **When port mode is 6x40G (default)** xe-1/1/3 • **When port mode is 4x100G** This port is not available.	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** This port is not available.

28	• **When port mode is 6x40G (default)** xe-1/1/4 • **When port mode is 4x100G** This port is not available.	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** This port is not available.
29	• **When port mode is 6x40G (default)** xe-1/1/5 • **When port mode is 4x100G** xe-1/1/3	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	• **When port mode is 6x40G (default)** xe-1/1/6 • **When port mode is 4x100G** xe-1/1/4	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	te-1/1/31	10Gb/s,1Gb/s, 100Mb/s
32	te-1/1/32	10Gb/s,1Gb/s, 100Mb/s
33	te-1/1/33	10Gb/s,1Gb/s, 100Mb/s
34	te-1/1/34	10Gb/s,1Gb/s, 100Mb/s
35	te-1/1/35	10Gb/s,1Gb/s, 100Mb/s
36	te-1/1/36	10Gb/s,1Gb/s, 100Mb/s
37	te-1/1/37	10Gb/s,1Gb/s, 100Mb/s
38	te-1/1/38	10Gb/s,1Gb/s, 100Mb/s
39	te-1/1/39	10Gb/s,1Gb/s, 100Mb/s
40	te-1/1/40	10Gb/s,1Gb/s, 100Mb/s
41	te-1/1/41	10Gb/s,1Gb/s, 100Mb/s
42	te-1/1/42	10Gb/s,1Gb/s, 100Mb/s
43	te-1/1/43	10Gb/s,1Gb/s, 100Mb/s
44	te-1/1/44	10Gb/s,1Gb/s, 100Mb/s
45	te-1/1/45	10Gb/s,1Gb/s, 100Mb/s
46	te-1/1/46	10Gb/s,1Gb/s, 100Mb/s
47	te-1/1/47	10Gb/s,1Gb/s, 100Mb/s
48	te-1/1/48	10Gb/s,1Gb/s, 100Mb/s
49	te-1/1/49	10Gb/s,1Gb/s, 100Mb/s
50	te-1/1/50	10Gb/s,1Gb/s, 100Mb/s
51	te-1/1/51	10Gb/s,1Gb/s, 100Mb/s
52	te-1/1/52	10Gb/s,1Gb/s, 100Mb/s
53	te-1/1/53	10Gb/s,1Gb/s, 100Mb/s
54	te-1/1/54	10Gb/s,1Gb/s, 100Mb/s

S5212F-ON Switch Port Name Description

Mapping between physical ports, interface names and interface supported speeds are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

S5224F-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

S5232F-ON Switch Port Name Description

NOTE:
On S5232F-ON switch, due to ASIC limitations, xe-1/1/32 port is not allowed to be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	te-1/1/1	10Gb/s,1Gb/s
34	te-1/1/2	10Gb/s,1Gb/s

S5248F Switch Port Name Description

NOTE:

1. The first 48 ports are grouped, each four ports are grouped as shown in the following table.

Groups of ports	port1- port4	port5- port8	port9- port12	port13- port16	port17- port20	port21- port24
	port25- port28	port29- port32	port33- port36	port37- port40	port41- port44	port45- port48

2. For the first 48 ports, the transmission rates of optical modules inserted in the ports of a group needs to be the same, and the configured port speed must be the same too, that is to say,

- when inserting an optical module to the switch port, the transmission rates of the optical modules should be the same in a group.
- you should manually configure the port speed by using the **set interface gigabit-ethernet speed** command before inserting an optical module, and the port speed of the four ports in the same group should be configured together and with the same value.

3. There are two 200G QSFP-DD ports, they should be inserted a 200G optical module. Each of the QSFP-DD port can be used as two separate 100G QSFP28 ports. The port name of the two 200G QSFP-DD ports are xe-1/1/1, xe-1/1/2, xe-1/1/3 and xe-1/1/4.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s

30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s
32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
55	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
56	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

S5296F-ON Switch Port Name Description

NOTE:

1. The first 96 ports are grouped, each four ports are grouped as shown in the following table.

Groups of ports	port1- port4	port5- port8	port9- port12	port13- port16	port17- port20	port21- port24
	port25- port28	port29- port32	port33- port36	port37- port40	port41- port44	port45- port48
	port49-port52	port53-port56	port57-port60	port61-port64	port65-port68	port69-port72
	port73-port76	port77-port80	port81-port84	port85-port88	port89-port92	port93-port96

2. For the first 96 ports, you should manually configure the port speed by using the **set interface gigabit-ethernet speed** command before inserting the cable and the port speed of the four ports in the same group should be configured together and with the same value.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s
30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s

32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	te-1/1/49	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/50	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/51	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/52	25Gb/s,10Gb/s,1Gb/s
53	te-1/1/53	25Gb/s,10Gb/s,1Gb/s
54	te-1/1/54	25Gb/s,10Gb/s,1Gb/s
55	te-1/1/55	25Gb/s,10Gb/s,1Gb/s
56	te-1/1/56	25Gb/s,10Gb/s,1Gb/s
57	te-1/1/57	25Gb/s,10Gb/s,1Gb/s
58	te-1/1/58	25Gb/s,10Gb/s,1Gb/s
59	te-1/1/59	25Gb/s,10Gb/s,1Gb/s
60	te-1/1/60	25Gb/s,10Gb/s,1Gb/s
61	te-1/1/61	25Gb/s,10Gb/s,1Gb/s
62	te-1/1/62	25Gb/s,10Gb/s,1Gb/s
63	te-1/1/63	25Gb/s,10Gb/s,1Gb/s
64	te-1/1/64	25Gb/s,10Gb/s,1Gb/s
65	te-1/1/65	25Gb/s,10Gb/s,1Gb/s
66	te-1/1/66	25Gb/s,10Gb/s,1Gb/s
67	te-1/1/67	25Gb/s,10Gb/s,1Gb/s
68	te-1/1/68	25Gb/s,10Gb/s,1Gb/s
69	te-1/1/69	25Gb/s,10Gb/s,1Gb/s
70	te-1/1/70	25Gb/s,10Gb/s,1Gb/s
71	te-1/1/71	25Gb/s,10Gb/s,1Gb/s
72	te-1/1/72	25Gb/s,10Gb/s,1Gb/s
73	te-1/1/73	25Gb/s,10Gb/s,1Gb/s
74	te-1/1/74	25Gb/s,10Gb/s,1Gb/s
75	te-1/1/75	25Gb/s,10Gb/s,1Gb/s
76	te-1/1/76	25Gb/s,10Gb/s,1Gb/s

77	te-1/1/77	25Gb/s,10Gb/s,1Gb/s
78	te-1/1/78	25Gb/s,10Gb/s,1Gb/s
79	te-1/1/79	25Gb/s,10Gb/s,1Gb/s
80	te-1/1/80	25Gb/s,10Gb/s,1Gb/s
81	te-1/1/81	25Gb/s,10Gb/s,1Gb/s
82	te-1/1/82	25Gb/s,10Gb/s,1Gb/s
83	te-1/1/83	25Gb/s,10Gb/s,1Gb/s
84	te-1/1/84	25Gb/s,10Gb/s,1Gb/s
85	te-1/1/85	25Gb/s,10Gb/s,1Gb/s
86	te-1/1/86	25Gb/s,10Gb/s,1Gb/s
87	te-1/1/87	25Gb/s,10Gb/s,1Gb/s
88	te-1/1/88	25Gb/s,10Gb/s,1Gb/s
89	te-1/1/89	25Gb/s,10Gb/s,1Gb/s
90	te-1/1/90	25Gb/s,10Gb/s,1Gb/s
91	te-1/1/91	25Gb/s,10Gb/s,1Gb/s
92	te-1/1/92	25Gb/s,10Gb/s,1Gb/s
93	te-1/1/93	25Gb/s,10Gb/s,1Gb/s
94	te-1/1/94	25Gb/s,10Gb/s,1Gb/s
95	te-1/1/95	25Gb/s,10Gb/s,1Gb/s
96	te-1/1/96	25Gb/s,10Gb/s,1Gb/s
97	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
98	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
99	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
100	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
101	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
102	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
103	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
104	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

Z9100-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of Z9100-ON are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/32	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	te-1/1/1	10Gb/s, 1Gb/s, 100Mb/s
54	te-1/1/2	10Gb/s, 1Gb/s, 100Mb/s

Z9264F-ON Switch Port Name Description

NOTE:
Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface supported speed on Z9264F-ON are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	xe-1/1/33	100Gb/s, 40Gb/s
34	xe-1/1/34	100Gb/s, 40Gb/s
35	xe-1/1/35	100Gb/s, 40Gb/s
36	xe-1/1/36	100Gb/s, 40Gb/s

37	xe-1/1/37	100Gb/s, 40Gb/s
38	xe-1/1/38	100Gb/s, 40Gb/s
39	xe-1/1/39	100Gb/s, 40Gb/s
40	xe-1/1/40	100Gb/s, 40Gb/s
41	xe-1/1/41	100Gb/s, 40Gb/s
42	xe-1/1/42	100Gb/s, 40Gb/s
43	xe-1/1/43	100Gb/s, 40Gb/s
44	xe-1/1/44	100Gb/s, 40Gb/s
45	xe-1/1/45	100Gb/s, 40Gb/s
46	xe-1/1/46	100Gb/s, 40Gb/s
47	xe-1/1/47	100Gb/s, 40Gb/s
48	xe-1/1/48	100Gb/s, 40Gb/s
49	xe-1/1/49	100Gb/s, 40Gb/s
50	xe-1/1/50	100Gb/s, 40Gb/s
51	xe-1/1/51	100Gb/s, 40Gb/s
52	xe-1/1/52	100Gb/s, 40Gb/s
53	xe-1/1/53	100Gb/s, 40Gb/s
54	xe-1/1/54	100Gb/s, 40Gb/s
55	xe-1/1/55	100Gb/s, 40Gb/s
56	xe-1/1/56	100Gb/s, 40Gb/s
57	xe-1/1/57	100Gb/s, 40Gb/s
58	xe-1/1/58	100Gb/s, 40Gb/s
59	xe-1/1/59	100Gb/s, 40Gb/s
60	xe-1/1/60	100Gb/s, 40Gb/s
61	xe-1/1/61	100Gb/s, 40Gb/s
62	xe-1/1/62	100Gb/s, 40Gb/s
63	xe-1/1/63	100Gb/s, 40Gb/s
64	xe-1/1/64	100Gb/s, 40Gb/s
65	te-1/1/1	10Gb/s
66	te-1/1/2	10Gb/s

S4128F-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of S4128F-ON are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s

S4128T-ON Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of S4128F-ON are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s, 100Mb/s
2	te-1/1/2	10Gb/s, 1Gb/s, 100Mb/s
3	te-1/1/3	10Gb/s, 1Gb/s, 100Mb/s
4	te-1/1/4	10Gb/s, 1Gb/s, 100Mb/s
5	te-1/1/5	10Gb/s, 1Gb/s, 100Mb/s
6	te-1/1/6	10Gb/s, 1Gb/s, 100Mb/s
7	te-1/1/7	10Gb/s, 1Gb/s, 100Mb/s
8	te-1/1/8	10Gb/s, 1Gb/s, 100Mb/s
9	te-1/1/9	10Gb/s, 1Gb/s, 100Mb/s
10	te-1/1/10	10Gb/s, 1Gb/s, 100Mb/s
11	te-1/1/11	10Gb/s, 1Gb/s, 100Mb/s
12	te-1/1/12	10Gb/s, 1Gb/s, 100Mb/s
13	te-1/1/13	10Gb/s, 1Gb/s, 100Mb/s
14	te-1/1/14	10Gb/s, 1Gb/s, 100Mb/s
15	te-1/1/15	10Gb/s, 1Gb/s, 100Mb/s
16	te-1/1/16	10Gb/s, 1Gb/s, 100Mb/s
17	te-1/1/17	10Gb/s, 1Gb/s, 100Mb/s
18	te-1/1/18	10Gb/s, 1Gb/s, 100Mb/s
19	te-1/1/19	10Gb/s, 1Gb/s, 100Mb/s
20	te-1/1/20	10Gb/s, 1Gb/s, 100Mb/s
21	te-1/1/21	10Gb/s, 1Gb/s, 100Mb/s
22	te-1/1/22	10Gb/s, 1Gb/s, 100Mb/s
23	te-1/1/23	10Gb/s, 1Gb/s, 100Mb/s
24	te-1/1/24	10Gb/s, 1Gb/s, 100Mb/s
25	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

27	te-1/1/27	10Gb/s, 1Gb/s, 100Mb/s
28	te-1/1/28	10Gb/s, 1Gb/s, 100Mb/s
29	te-1/1/29	10Gb/s, 1Gb/s, 100Mb/s
30	te-1/1/30	10Gb/s, 1Gb/s, 100Mb/s

S4148F-ON Switch Port Name Description

NOTEs:

The uplink ports, with port numbers from 25 to 30, have two different uplink port modes 6x40G (default) and 4x100G.

- You need to change the port mode to 4x100G if you want to use 100G uplinks, please refer to following page with instructions to set up the port mode:

Configuring Port Mapping On S4148 Series Switch

- Ports with physical port number 27 & 28 are only available in the 6x40G mode and are not available in the 4x100G mode.

Mapping between physical ports, interface names and interface support speed of S4148F-ON are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s,1Gb/s
2	te-1/1/2	10Gb/s,1Gb/s
3	te-1/1/3	10Gb/s,1Gb/s
4	te-1/1/4	10Gb/s,1Gb/s
5	te-1/1/5	10Gb/s,1Gb/s
6	te-1/1/6	10Gb/s,1Gb/s
7	te-1/1/7	10Gb/s,1Gb/s
8	te-1/1/8	10Gb/s,1Gb/s
9	te-1/1/9	10Gb/s,1Gb/s
10	te-1/1/10	10Gb/s,1Gb/s
11	te-1/1/11	10Gb/s,1Gb/s
12	te-1/1/12	10Gb/s,1Gb/s
13	te-1/1/13	10Gb/s,1Gb/s
14	te-1/1/14	10Gb/s,1Gb/s
15	te-1/1/15	10Gb/s,1Gb/s
16	te-1/1/16	10Gb/s,1Gb/s
17	te-1/1/17	10Gb/s,1Gb/s
18	te-1/1/18	10Gb/s,1Gb/s
19	te-1/1/19	10Gb/s,1Gb/s
20	te-1/1/20	10Gb/s,1Gb/s

21	te-1/1/21	10Gb/s,1Gb/s
22	te-1/1/22	10Gb/s,1Gb/s
23	te-1/1/23	10Gb/s,1Gb/s
24	te-1/1/24	10Gb/s,1Gb/s
25	• **When port mode is 6x40G (default)** xe-1/1/1 • **When port mode is 4x100G** xe-1/1/1	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	• **When port mode is 6x40G (default)** xe-1/1/2 • **When port mode is 4x100G** xe-1/1/2	• **When port mode is 6x40G (default)** • 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** • 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	• **When port mode is 6x40G (default)** xe-1/1/3 • **When port mode is 4x100G** This port is not available.	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** This port is not available.
28	• **When port mode is 6x40G (default)** xe-1/1/4 • **When port mode is 4x100G** This port is not available.	• **When port mode is 6x40G (default)** 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** This port is not available.
29	• **When port mode is 6x40G (default)** xe-1/1/5 • **When port mode is 4x100G** xe-1/1/3	• **When port mode is 6x40G (default)** • 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** • 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	• **When port mode is 6x40G (default)** xe-1/1/6 • **When port mode is 4x100G** xe-1/1/4	• **When port mode is 6x40G (default)** • 40Gb/s, 4x10Gb/s, 4x1Gb/s • **When port mode is 4x100G** • 100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	te-1/1/31	10Gb/s,1Gb/s
32	te-1/1/32	10Gb/s,1Gb/s
33	te-1/1/33	10Gb/s,1Gb/s
34	te-1/1/34	10Gb/s,1Gb/s
35	te-1/1/35	10Gb/s,1Gb/s
36	te-1/1/36	10Gb/s,1Gb/s

37	te-1/1/37	10Gb/s,1Gb/s
38	te-1/1/38	10Gb/s,1Gb/s
39	te-1/1/39	10Gb/s,1Gb/s
40	te-1/1/40	10Gb/s,1Gb/s
41	te-1/1/41	10Gb/s,1Gb/s
42	te-1/1/42	10Gb/s,1Gb/s
43	te-1/1/43	10Gb/s,1Gb/s
44	te-1/1/44	10Gb/s,1Gb/s
45	te-1/1/45	10Gb/s,1Gb/s
46	te-1/1/46	10Gb/s,1Gb/s
47	te-1/1/47	10Gb/s,1Gb/s
48	te-1/1/48	10Gb/s,1Gb/s
49	te-1/1/49	10Gb/s,1Gb/s
50	te-1/1/50	10Gb/s,1Gb/s
51	te-1/1/51	10Gb/s,1Gb/s
52	te-1/1/52	10Gb/s,1Gb/s
53	te-1/1/53	10Gb/s,1Gb/s
54	te-1/1/54	10Gb/s,1Gb/s

EdgeCore/Accton Switch Port Name Description

- AS5812_54T/AS5812_54X Switch Port Name Description
- AS4625-54P/AS4625-54T Switch Port Name Description
- AS4630-54NPE Switch Port Name Description
- AS4630-54PE Switch Port Name Description
- AS6812_32X Switch Port Name Description
- AS7312-54X/AS7312_54XS Switch Port Name Description
- AS7326-56X Switch Port Name Description
- AS7726-32X Switch Port Name Description
- AS7816-64X Switch Port Name Description
- AS9716-32D Switch Port Name Description
- AS4610_30T/AS4610_30P Switch Port Name Description
- AS4610_54T/AS4610_54P Switch Port Name Description
- AS5712_54X Switch Port Name Description
- AS5835_54X/AS5835_54T Switch Port Name Description
- AS7712_32X Switch Port Name Description

AS5812_54T/AS5812_54X Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of AS5812_54T/AS5812_54X are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s

27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
50	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
51	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
52	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
53	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s

AS4625-54P/AS4625-54T Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	10/100/1000M
2	ge-1/1/2	10/100/1000M
3	ge-1/1/3	10/100/1000M
4	ge-1/1/4	10/100/1000M
5	ge-1/1/5	10/100/1000M
6	ge-1/1/6	10/100/1000M
7	ge-1/1/7	10/100/1000M
8	ge-1/1/8	10/100/1000M
9	ge-1/1/9	10/100/1000M
10	ge-1/1/10	10/100/1000M
11	ge-1/1/11	10/100/1000M
12	ge-1/1/12	10/100/1000M
13	ge-1/1/13	10/100/1000M
14	ge-1/1/14	10/100/1000M
15	ge-1/1/15	10/100/1000M
16	ge-1/1/16	10/100/1000M
17	ge-1/1/17	10/100/1000M
18	ge-1/1/18	10/100/1000M
19	ge-1/1/19	10/100/1000M
20	ge-1/1/20	10/100/1000M
21	ge-1/1/21	10/100/1000M
22	ge-1/1/22	10/100/1000M
23	ge-1/1/23	10/100/1000M
24	ge-1/1/24	10/100/1000M
25	ge-1/1/25	10/100/1000M
26	ge-1/1/26	10/100/1000M
27	ge-1/1/27	10/100/1000M
28	ge-1/1/28	10/100/1000M
29	ge-1/1/29	10/100/1000M
30	ge-1/1/30	10/100/1000M
31	ge-1/1/31	10/100/1000M
32	ge-1/1/32	10/100/1000M
33	ge-1/1/33	10/100/1000M
34	ge-1/1/34	10/100/1000M
35	ge-1/1/35	10/100/1000M
36	ge-1/1/36	10/100/1000M
37	ge-1/1/37	10/100/1000M
38	ge-1/1/38	10/100/1000M
39	ge-1/1/39	10/100/1000M

40	ge-1/1/40	10/100/1000M
41	ge-1/1/41	10/100/1000M
42	ge-1/1/42	10/100/1000M
43	ge-1/1/43	10/100/1000M
44	ge-1/1/44	10/100/1000M
45	ge-1/1/45	10/100/1000M
46	ge-1/1/46	10/100/1000M
47	ge-1/1/47	10/100/1000M
48	ge-1/1/48	10/100/1000M
49	te-1/1/1	10G, 1G
50	te-1/1/2	10G, 1G
51	te-1/1/3	10G, 1G
52	te-1/1/4	10G, 1G
53	te-1/1/5	10G, 1G
54	te-1/1/6	10G, 1G

AS4630-54NPE Switch Port Name Description

NOTE:
Ports Te-1/1/1, Te-1/1/2, Te-1/1/3 and Te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not Allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note: If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	2.5 Gb/s, 1 Gb/s, 100Mb/s
2	ge-1/1/2	2.5 Gb/s, 1 Gb/s, 100Mb/s
3	ge-1/1/3	2.5 Gb/s, 1 Gb/s, 100Mb/s
4	ge-1/1/4	2.5 Gb/s, 1 Gb/s, 100Mb/s
5	ge-1/1/5	2.5 Gb/s, 1 Gb/s, 100Mb/s
6	ge-1/1/6	2.5 Gb/s, 1 Gb/s, 100Mb/s
7	ge-1/1/7	2.5 Gb/s, 1 Gb/s, 100Mb/s
8	ge-1/1/8	2.5 Gb/s, 1 Gb/s, 100Mb/s
9	ge-1/1/9	2.5 Gb/s, 1 Gb/s, 100Mb/s
10	ge-1/1/10	2.5 Gb/s, 1 Gb/s, 100Mb/s
11	ge-1/1/11	2.5 Gb/s, 1 Gb/s, 100Mb/s
12	ge-1/1/12	2.5 Gb/s, 1 Gb/s, 100Mb/s
13	ge-1/1/13	2.5 Gb/s, 1 Gb/s, 100Mb/s
14	ge-1/1/14	2.5 Gb/s, 1 Gb/s, 100Mb/s
15	ge-1/1/15	2.5 Gb/s, 1 Gb/s, 100Mb/s
16	ge-1/1/16	2.5 Gb/s, 1 Gb/s, 100Mb/s
17	ge-1/1/17	2.5 Gb/s, 1 Gb/s, 100Mb/s
18	ge-1/1/18	2.5 Gb/s, 1 Gb/s, 100Mb/s
19	ge-1/1/19	2.5 Gb/s, 1 Gb/s, 100Mb/s
20	ge-1/1/20	2.5 Gb/s, 1 Gb/s, 100Mb/s
21	ge-1/1/21	2.5 Gb/s, 1 Gb/s, 100Mb/s
22	ge-1/1/22	2.5 Gb/s, 1 Gb/s, 100Mb/s
23	ge-1/1/23	2.5 Gb/s, 1 Gb/s, 100Mb/s
24	ge-1/1/24	2.5 Gb/s, 1 Gb/s, 100Mb/s
25	ge-1/1/25	2.5 Gb/s, 1 Gb/s, 100Mb/s
26	ge-1/1/26	2.5 Gb/s, 1 Gb/s, 100Mb/s

27	ge-1/1/27	2.5 Gb/s, 1 Gb/s, 100Mb/s
28	ge-1/1/28	2.5 Gb/s, 1 Gb/s, 100Mb/s
29	ge-1/1/29	2.5 Gb/s, 1 Gb/s, 100Mb/s
30	ge-1/1/30	2.5 Gb/s, 1 Gb/s, 100Mb/s
31	ge-1/1/31	2.5 Gb/s, 1 Gb/s, 100Mb/s
32	ge-1/1/32	2.5 Gb/s, 1 Gb/s, 100Mb/s
33	ge-1/1/33	2.5 Gb/s, 1 Gb/s, 100Mb/s
34	ge-1/1/34	2.5 Gb/s, 1 Gb/s, 100Mb/s
35	ge-1/1/35	2.5 Gb/s, 1 Gb/s, 100Mb/s
36	ge-1/1/36	2.5 Gb/s, 1 Gb/s, 100Mb/s
37	ge-1/1/37	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
38	ge-1/1/38	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
39	ge-1/1/39	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
40	ge-1/1/40	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
41	ge-1/1/41	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
42	ge-1/1/42	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
43	ge-1/1/43	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
44	ge-1/1/44	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
45	ge-1/1/45	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
46	ge-1/1/46	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
47	ge-1/1/47	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
48	ge-1/1/48	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

AS4630-54PE Switch Port Name Description

NOTE:
Ports Te-1/1/1, Te-1/1/2, Te-1/1/3 and Te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not Allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note: If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	1Gb/s, 100Mb/s, 10Mb/s
2	ge-1/1/2	1Gb/s, 100Mb/s, 10Mb/s
3	ge-1/1/3	1Gb/s, 100Mb/s, 10Mb/s
4	ge-1/1/4	1Gb/s, 100Mb/s, 10Mb/s
5	ge-1/1/5	1Gb/s, 100Mb/s, 10Mb/s
6	ge-1/1/6	1Gb/s, 100Mb/s, 10Mb/s
7	ge-1/1/7	1Gb/s, 100Mb/s, 10Mb/s
8	ge-1/1/8	1Gb/s, 100Mb/s, 10Mb/s
9	ge-1/1/9	1Gb/s, 100Mb/s, 10Mb/s
10	ge-1/1/10	1Gb/s, 100Mb/s, 10Mb/s
11	ge-1/1/11	1Gb/s, 100Mb/s, 10Mb/s
12	ge-1/1/12	1Gb/s, 100Mb/s, 10Mb/s
13	ge-1/1/13	1Gb/s, 100Mb/s, 10Mb/s
14	ge-1/1/14	1Gb/s, 100Mb/s, 10Mb/s
15	ge-1/1/15	1Gb/s, 100Mb/s, 10Mb/s
16	ge-1/1/16	1Gb/s, 100Mb/s, 10Mb/s
17	ge-1/1/17	1Gb/s, 100Mb/s, 10Mb/s
18	ge-1/1/18	1Gb/s, 100Mb/s, 10Mb/s
19	ge-1/1/19	1Gb/s, 100Mb/s, 10Mb/s
20	ge-1/1/20	1Gb/s, 100Mb/s, 10Mb/s
21	ge-1/1/21	1Gb/s, 100Mb/s, 10Mb/s
22	ge-1/1/22	1Gb/s, 100Mb/s, 10Mb/s
23	ge-1/1/23	1Gb/s, 100Mb/s, 10Mb/s
24	ge-1/1/24	1Gb/s, 100Mb/s, 10Mb/s
25	ge-1/1/25	1Gb/s, 100Mb/s, 10Mb/s
26	ge-1/1/26	1Gb/s, 100Mb/s, 10Mb/s

Physical Port Number	Interface Names	Interface Supported Speed
27	ge-1/1/27	1Gb/s, 100Mb/s, 10Mb/s
28	ge-1/1/28	1Gb/s, 100Mb/s, 10Mb/s
29	ge-1/1/29	1Gb/s, 100Mb/s, 10Mb/s
30	ge-1/1/30	1Gb/s, 100Mb/s, 10Mb/s
31	ge-1/1/31	1Gb/s, 100Mb/s, 10Mb/s
32	ge-1/1/32	1Gb/s, 100Mb/s, 10Mb/s
33	ge-1/1/33	1Gb/s, 100Mb/s, 10Mb/s
34	ge-1/1/34	1Gb/s, 100Mb/s, 10Mb/s
35	ge-1/1/35	1Gb/s, 100Mb/s, 10Mb/s
36	ge-1/1/36	1Gb/s, 100Mb/s, 10Mb/s
37	ge-1/1/37	1Gb/s, 100Mb/s, 10Mb/s
38	ge-1/1/38	1Gb/s, 100Mb/s, 10Mb/s
39	ge-1/1/39	1Gb/s, 100Mb/s, 10Mb/s
40	ge-1/1/40	1Gb/s, 100Mb/s, 10Mb/s
41	ge-1/1/41	1Gb/s, 100Mb/s, 10Mb/s
42	ge-1/1/42	1Gb/s, 100Mb/s, 10Mb/s
43	ge-1/1/43	1Gb/s, 100Mb/s, 10Mb/s
44	ge-1/1/44	1Gb/s, 100Mb/s, 10Mb/s
45	ge-1/1/45	1Gb/s, 100Mb/s, 10Mb/s
46	ge-1/1/46	1Gb/s, 100Mb/s, 10Mb/s
47	ge-1/1/47	1Gb/s, 100Mb/s, 10Mb/s
48	ge-1/1/48	1Gb/s, 100Mb/s, 10Mb/s
49	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

AS6812_32X Switch Port Name Description

NOTE:

Due to hardware limitations, ports xe-1/1/13, xe-1/1/14, xe-1/1/15, xe-1/1/16, xe-1/1/29, xe-1/1/30, xe-1/1/31 and xe-1/1/32 are not allowed to be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
2	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
3	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
4	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
5	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
6	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s
7	xe-1/1/7	40Gb/s, 4x10Gb/s, 4x1Gb/s
8	xe-1/1/8	40Gb/s, 4x10Gb/s, 4x1Gb/s
9	xe-1/1/9	40Gb/s, 4x10Gb/s, 4x1Gb/s
10	xe-1/1/10	40Gb/s, 4x10Gb/s, 4x1Gb/s
11	xe-1/1/11	40Gb/s, 4x10Gb/s, 4x1Gb/s
12	xe-1/1/12	40Gb/s, 4x10Gb/s, 4x1Gb/s
13	xe-1/1/13	40Gb/s
14	xe-1/1/14	40Gb/s
15	xe-1/1/15	40Gb/s
16	xe-1/1/16	40Gb/s
17	xe-1/1/17	40Gb/s, 4x10Gb/s, 4x1Gb/s
18	xe-1/1/18	40Gb/s, 4x10Gb/s, 4x1Gb/s
19	xe-1/1/19	40Gb/s, 4x10Gb/s, 4x1Gb/s
20	xe-1/1/20	40Gb/s, 4x10Gb/s, 4x1Gb/s
21	xe-1/1/21	40Gb/s, 4x10Gb/s, 4x1Gb/s
22	xe-1/1/22	40Gb/s, 4x10Gb/s, 4x1Gb/s
23	xe-1/1/23	40Gb/s, 4x10Gb/s, 4x1Gb/s
24	xe-1/1/24	40Gb/s, 4x10Gb/s, 4x1Gb/s
25	xe-1/1/25	40Gb/s, 4x10Gb/s, 4x1Gb/s
26	xe-1/1/26	40Gb/s, 4x10Gb/s, 4x1Gb/s
27	xe-1/1/27	40Gb/s, 4x10Gb/s, 4x1Gb/s
28	xe-1/1/28	40Gb/s, 4x10Gb/s, 4x1Gb/s
29	xe-1/1/29	40Gb/s
30	xe-1/1/30	40Gb/s
31	xe-1/1/31	40Gb/s
32	xe-1/1/32	40Gb/s

AS7312-54X/AS7312_54XS Switch Port Name Description

NOTE:
Follow the below precautions before using AS7312_54X/AS7312_54XS switch:

1. The first 48 ports are grouped, each four ports are grouped as shown in the following table.

Groups of ports	port1- port4	port5- port8	port9- port12	port13- port16	port17- port20	port21- port24
	port25- port28	port29- port32	port33- port36	port37- port40	port41- port44	port45- port48

2. When configuring the port rate, the supported rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports in the same group can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for the group of ports.

	te-1/1/21	**te-1/1/22**	**te-1/1/23**	**te-1/1/24**	**Allowed or not allowed**
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s

24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s
30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s
32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

AS7326-56X Switch Port Name Description

NOTE:

1. The first 48 ports are grouped as shown in the following table, four ports form a group.

Group	Ports
1	Port1, Port2, Port3, Port6
2	Port4, Port5, Port7, Port9
3	Port8, Port10, Port11, Port12
4	Port13, Port14, Port15, Port18
5	Port16, Port17, Port19, Port21
6	Port20, Port22, Port23, Port24
7	Port25, Port26, Port27, Port30
8	Port28, Port29, Port31, Port33
9	Port32, Port34, Port35, Port36
10	Port37, Port38, Port39, Port42
11	Port40, Port41, Port43, Port45
12	Port44, Port46, Port47, Port48

2. For the first 48 ports, the transmission rates of optical modules inserted in the ports of a group needs to be the same, and the configured port speed must be the same too, that is to say,

- when inserting an optical module to the switch port, the transmission rates of the optical modules should be the same in a group.
- you should manually configure the port speed by using the **set interface gigabit-ethernet speed** command before inserting an optical module, and the port speed of the four ports in the same group should be configured together and with the same value.

3. The last two ports are 10G-Base-KR ports which can be configured as two 10G SFP+ ports on the front panel or two 10G-KR ports linked to CPU. By default, 10G-Base-KR ports are disabled. For details please refer to document 10G-Base-KR Interface Configuration.

4. On AS7326-56X switch, when the 10G-Base-KR ports are enabled as either front panel ports or management ports, xe-1/1/8 port is not allowed to be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s

17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s
30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s
32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
55	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
56	xe-1/1/8	100Gb/s,40Gb/s, 4x25Gb/s, 4x10Gb/s
57	me-1/1/1(Management Port)	auto
	te-1/1/49(Front Panel Port)	10Gb/s,1Gb/s
58	me-1/1/2(Management Port)	auto
	te-1/1/50(Front Panel Port)	10Gb/s,1Gb/s

AS7726-32X Switch Port Name Description

NOTE:

- The last two ports are 10G-Base-KR ports which can be configured as two 10G SFP+ ports on the front panel or two 10G-KR ports linked to CPU. By default, 10G-Base-KR ports are disabled. For details please refer to document 10G-Base-KR Interface Configuration.
- On AS7726-32X switch, when the 10G-Base-KR ports are enabled as either front panel ports or management ports, xe-1/1/32 port is not allowed to be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	me-1/1/1(Management Port)	auto
	te-1/1/1(Front Panel Port)	10Gb/s,1Gb/s
34	me-1/1/2(Management Port)	auto

	te-1/1/2(Front Panel Port)	10Gb/s,1Gb/s

AS7816-64X Switch Port Name Description

NOTE:
Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface supported speed on AS7816-64X are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	xe-1/1/33	100Gb/s, 40Gb/s
34	xe-1/1/34	100Gb/s, 40Gb/s
35	xe-1/1/35	100Gb/s, 40Gb/s
36	xe-1/1/36	100Gb/s, 40Gb/s

37	xe-1/1/37	100Gb/s, 40Gb/s
38	xe-1/1/38	100Gb/s, 40Gb/s
39	xe-1/1/39	100Gb/s, 40Gb/s
40	xe-1/1/40	100Gb/s, 40Gb/s
41	xe-1/1/41	100Gb/s, 40Gb/s
42	xe-1/1/42	100Gb/s, 40Gb/s
43	xe-1/1/43	100Gb/s, 40Gb/s
44	xe-1/1/44	100Gb/s, 40Gb/s
45	xe-1/1/45	100Gb/s, 40Gb/s
46	xe-1/1/46	100Gb/s, 40Gb/s
47	xe-1/1/47	100Gb/s, 40Gb/s
48	xe-1/1/48	100Gb/s, 40Gb/s
49	xe-1/1/49	100Gb/s, 40Gb/s
50	xe-1/1/50	100Gb/s, 40Gb/s
51	xe-1/1/51	100Gb/s, 40Gb/s
52	xe-1/1/52	100Gb/s, 40Gb/s
53	xe-1/1/53	100Gb/s, 40Gb/s
54	xe-1/1/54	100Gb/s, 40Gb/s
55	xe-1/1/55	100Gb/s, 40Gb/s
56	xe-1/1/56	100Gb/s, 40Gb/s
57	xe-1/1/57	100Gb/s, 40Gb/s
58	xe-1/1/58	100Gb/s, 40Gb/s
59	xe-1/1/59	100Gb/s, 40Gb/s
60	xe-1/1/60	100Gb/s, 40Gb/s
61	xe-1/1/61	100Gb/s, 40Gb/s
62	xe-1/1/62	100Gb/s, 40Gb/s
63	xe-1/1/63	100Gb/s, 40Gb/s
64	xe-1/1/64	100Gb/s, 40Gb/s

AS9716-32D Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
2	xe-1/1/2	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
3	xe-1/1/3	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
4	xe-1/1/4	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
5	xe-1/1/5	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
6	xe-1/1/6	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
7	xe-1/1/7	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
8	xe-1/1/8	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
9	xe-1/1/9	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
10	xe-1/1/10	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
11	xe-1/1/11	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
12	xe-1/1/12	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
13	xe-1/1/13	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
14	xe-1/1/14	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
15	xe-1/1/15	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
16	xe-1/1/16	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
17	xe-1/1/17	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s

18	xe-1/1/18	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
19	xe-1/1/19	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
20	xe-1/1/20	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
21	xe-1/1/21	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
22	xe-1/1/22	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
23	xe-1/1/23	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
24	xe-1/1/24	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
25	xe-1/1/25	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
26	xe-1/1/26	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
27	xe-1/1/27	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
28	xe-1/1/28	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
29	xe-1/1/29	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
30	xe-1/1/30	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
31	xe-1/1/31	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s
32	xe-1/1/32	400Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s

AS4610_30T/AS4610_30P Switch Port Name Description

Mapping between physical ports, interface names and interface support speeds on ACCTON_AS4610_30T/ACCTON_AS4610_30P are displayed in the following table.

Physical Port Number	Interface Name In Normal Mode	Port Support Speed
1	ge-1/1/1	1Gb/s,100Mb/s and 10Mb/s
2	ge-1/1/2	1Gb/s,100Mb/s and 10Mb/s
3	ge-1/1/3	1Gb/s,100Mb/s and 10Mb/s
4	ge-1/1/4	1Gb/s,100Mb/s and 10Mb/s
5	ge-1/1/5	1Gb/s,100Mb/s and 10Mb/s
6	ge-1/1/6	1Gb/s,100Mb/s and 10Mb/s
7	ge-1/1/7	1Gb/s,100Mb/s and 10Mb/s
8	ge-1/1/8	1Gb/s,100Mb/s and 10Mb/s
9	ge-1/1/9	1Gb/s,100Mb/s and 10Mb/s
10	ge-1/1/10	1Gb/s,100Mb/s and 10Mb/s
11	ge-1/1/11	1Gb/s,100Mb/s and 10Mb/s
12	ge-1/1/12	1Gb/s,100Mb/s and 10Mb/s
13	ge-1/1/13	1Gb/s,100Mb/s and 10Mb/s
14	ge-1/1/14	1Gb/s,100Mb/s and 10Mb/s
15	ge-1/1/15	1Gb/s,100Mb/s and 10Mb/s
16	ge-1/1/16	1Gb/s,100Mb/s and 10Mb/s
17	ge-1/1/17	1Gb/s,100Mb/s and 10Mb/s
18	ge-1/1/18	1Gb/s,100Mb/s and 10Mb/s
19	ge-1/1/19	1Gb/s,100Mb/s and 10Mb/s
20	ge-1/1/20	1Gb/s,100Mb/s and 10Mb/s
21	ge-1/1/21	1Gb/s,100Mb/s and 10Mb/s
22	ge-1/1/22	1Gb/s,100Mb/s and 10Mb/s
23	ge-1/1/23	1Gb/s,100Mb/s and 10Mb/s
24	ge-1/1/24	1Gb/s,100Mb/s and 10Mb/s

25	te-1/1/1	10Gb/s and 1Gb/s
26	te-1/1/2	10Gb/s and 1Gb/s
27	te-1/1/3	10Gb/s and 1Gb/s
28	te-1/1/4	10Gb/s and 1Gb/s
29	te-1/1/5	20Gb/s
30	te-1/1/6	20Gb/s

NOTE:

Ports te-1/1/5 and te-1/1/6 cannot support 20G/s at this time.

.

AS4610_54T/AS4610_54P Switch Port Name Description

Mapping between physical ports, interface names and interface support speeds on AS4610_54T/AS4610_54P are displayed in the following table.

Physical Port Number	Interface Name	Port Support Speed
1	ge-1/1/1	1Gb/s,100Mb/s and 10Mb/s
2	ge-1/1/2	1Gb/s,100Mb/s and 10Mb/s
3	ge-1/1/3	1Gb/s,100Mb/s and 10Mb/s
4	ge-1/1/4	1Gb/s,100Mb/s and 10Mb/s
5	ge-1/1/5	1Gb/s,100Mb/s and 10Mb/s
6	ge-1/1/6	1Gb/s,100Mb/s and 10Mb/s
7	ge-1/1/7	1Gb/s,100Mb/s and 10Mb/s
8	ge-1/1/8	1Gb/s,100Mb/s and 10Mb/s
9	ge-1/1/9	1Gb/s,100Mb/s and 10Mb/s
10	ge-1/1/10	1Gb/s,100Mb/s and 10Mb/s
11	ge-1/1/11	1Gb/s,100Mb/s and 10Mb/s
12	ge-1/1/12	1Gb/s,100Mb/s and 10Mb/s
13	ge-1/1/13	1Gb/s,100Mb/s and 10Mb/s
14	ge-1/1/14	1Gb/s,100Mb/s and 10Mb/s
15	ge-1/1/15	1Gb/s,100Mb/s and 10Mb/s
16	ge-1/1/16	1Gb/s,100Mb/s and 10Mb/s
17	ge-1/1/17	1Gb/s,100Mb/s and 10Mb/s
18	ge-1/1/18	1Gb/s,100Mb/s and 10Mb/s
19	ge-1/1/19	1Gb/s,100Mb/s and 10Mb/s
20	ge-1/1/20	1Gb/s,100Mb/s and 10Mb/s
21	ge-1/1/21	1Gb/s,100Mb/s and 10Mb/s
22	ge-1/1/22	1Gb/s,100Mb/s and 10Mb/s
23	ge-1/1/23	1Gb/s,100Mb/s and 10Mb/s
24	ge-1/1/24	1Gb/s,100Mb/s and 10Mb/s

25	ge-1/1/25	1Gb/s,100Mb/s and 10Mb/s
26	ge-1/1/26	1Gb/s,100Mb/s and 10Mb/s
27	ge-1/1/27	1Gb/s,100Mb/s and 10Mb/s
28	ge-1/1/28	1Gb/s,100Mb/s and 10Mb/s
29	ge-1/1/29	1Gb/s,100Mb/s and 10Mb/s
30	ge-1/1/30	1Gb/s,100Mb/s and 10Mb/s
31	ge-1/1/31	1Gb/s,100Mb/s and 10Mb/s
32	ge-1/1/32	1Gb/s,100Mb/s and 10Mb/s
33	ge-1/1/33	1Gb/s,100Mb/s and 10Mb/s
34	ge-1/1/34	1Gb/s,100Mb/s and 10Mb/s
35	ge-1/1/35	1Gb/s,100Mb/s and 10Mb/s
36	ge-1/1/36	1Gb/s,100Mb/s and 10Mb/s
37	ge-1/1/37	1Gb/s,100Mb/s and 10Mb/s
38	ge-1/1/38	1Gb/s,100Mb/s and 10Mb/s
39	ge-1/1/39	1Gb/s,100Mb/s and 10Mb/s
40	ge-1/1/40	1Gb/s,100Mb/s and 10Mb/s
41	ge-1/1/41	1Gb/s,100Mb/s and 10Mb/s
42	ge-1/1/42	1Gb/s,100Mb/s and 10Mb/s
43	ge-1/1/43	1Gb/s,100Mb/s and 10Mb/s
44	ge-1/1/44	1Gb/s,100Mb/s and 10Mb/s
45	ge-1/1/45	1Gb/s,100Mb/s and 10Mb/s
46	ge-1/1/46	1Gb/s,100Mb/s and 10Mb/s
47	ge-1/1/47	1Gb/s,100Mb/s and 10Mb/s
48	ge-1/1/48	1Gb/s,100Mb/s and 10Mb/s
49	te-1/1/1	10Gb/s and 1Gb/s
50	te-1/1/2	10Gb/s and 1Gb/s
51	te-1/1/3	10Gb/s and 1Gb/s
52	te-1/1/4	10Gb/s and 1Gb/s
53	te-1/1/5	20Gb/s
54	te-1/1/6	20Gb/s



Note

Ports te-1/1/5 and te-1/1/6 cannot support 20G/s at this time.

AS5712_54X Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of AS5712_54X are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s

27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
50	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
51	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
52	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
53	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s

AS5835_54X/AS5835_54T Switch Port Name Description

NOTE:

Due to hardware limitations, only ports xe-1/1/1 and xe-1/1/4 support to be split into four Gigabit Ethernet interfaces, other ports are not supported to be split.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s

25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s
27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s

AS7712_32X Switch Port Name Description

Mapping between physical ports, interface names and interface support speed on AS7712_32X are shown in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

Delta/Agema Switch Port Name Description

- AG5648V1 Switch Port Name Description
- AG7648 Switch Port Name Description
- AG9032v1 Switch Port Name Description

AG5648V1 Switch Port Name Description

NOTE:
Follow the below precautions before using AG5648 switch:

1. The first 48 ports are grouped, each four ports are grouped as shown in the following table.

Groups of ports	port1- port4	port5- port8	port9- port12	port13- port16	port17- port20	port21- port24
	port25- port28	port29- port32	port33- port36	port37- port40	port41- port44	port45- port48

2. When configuring the port rate, the supported rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports in the same group can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for the group of ports.

	te-1/1/21	**te-1/1/22**	**te-1/1/23**	**te-1/1/24**	**Allowed or not allowed**
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s
9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s

24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s
30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s
32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

AG7648 Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s
27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s

40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
50	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
51	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
52	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
53	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s

AG9032v1 Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

FS Switch Port Name Description

- N5850-48S6Q Switch Port Name Description
- N8550-32C Switch Port Name Description
- N8550-48B8C Switch Port Name Description
- S5810-48TS-P Switch Port Name Description
- S5810-28FS Switch Port Name Description
- S5810-28TS Switch Port Name Description
- S5810-48FS Switch Port Name Description
- S5810-48TS Switch Port Name Description
- S5860-20SQ Switch Port Name Description
- S5860-24XB-U Switch Port Name Description
- N8560-32C Switch Port Name Description
- N8560-64C Switch Port Name Description
- S5860-24MG-U Switch Port Name Description
- S5860-48XMG-U/S5860-48XMG Switch Port Name Description
- S5860-24XMG Switch Port Name Description
- S5860-48MG-U Switch Port Name Description
- S5870-48T6S-U/S5870-48T6S Switch Port Name Description
- S5870-48T6BC/S5870-48T6BC-U Switch Port Name Description
- N5850-48X6C Switch Port Name Description
- N8550-64C Switch Port Name Description
- N9550-32D Switch Port Name Description
- N5850-48S6C Switch Port Name Description
- S5870-48MX6BC-U Switch Port Name Description
- S3410-24TS Switch Port Name Description
- S3410L-24TF Switch Port Name Description
- S3410L-24TF-P Switch Port Name Description
- S3410-24TS-P Switch Port Name Description
- S3410C-16TMS-P Switch Port Name Description
- S3410C-16TF-P Switch Port Name Description
- S3410C-8TMS-P Switch Port Name Description
- S3410C-16TF Switch Port Name Description
- S3410-48TS-P Switch Port Name Description
- S3410-48TS Switch Port Name Description
- S3410L-48TF Switch Port Name Description
- N8550-24CD8D Switch Port Name Description
- N9600-64OD Switch Port Name Description

N5850-48S6Q Switch Port Name Description

Mapping between physical ports, interface names and interface support speed of N5850-48S6Q are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s
25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s

27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
50	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s
51	xe-1/1/3	40Gb/s, 4x10Gb/s, 4x1Gb/s
52	xe-1/1/4	40Gb/s, 4x10Gb/s, 4x1Gb/s
53	xe-1/1/5	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/6	40Gb/s, 4x10Gb/s, 4x1Gb/s

N8550-32C Switch Port Name Description

NOTE:

- The last two ports are 10G-Base-KR ports which can be configured as two 10G SFP+ ports on the front panel or two 10G-KR ports linked to CPU. By default, 10G-Base-KR ports are disabled. For details please refer to document 10G-Base-KR Interface Configuration.
- On N8550-32C switch, when the 10G-Base-KR ports are enabled as either front panel ports or management ports, xe-1/1/32 port is not allowed to be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	me-1/1/1(Management Port)	auto
	te-1/1/1(Front Panel Port)	10Gb/s,1Gb/s
34	me-1/1/2(Management Port)	auto

	te-1/1/2(Front Panel Port)	10Gb/s,1Gb/s

N8550-48B8C Switch Port Name Description

NOTEs:

1. The last two ports are 10G-Base-KR ports which can be configured as two 10G SFP+ ports on the front panel or two 10G-KR ports linked to CPU. By default, 10G-Base-KR ports are disabled. For details please refer to document 10G-Base-KR Interface Configuration.

2. On N8550-48B8C switch, when the 10G-Base-KR ports are enabled as either front panel ports or management ports, xe-1/1/8 port is not allowed to be split into four Gigabit Ethernet interfaces.

3. The first 48 ports are grouped as shown in the following table, four ports form a group.

Group	Ports
1	Port1, Port2, Port3, Port6
2	Port4, Port5, Port7, Port9
3	Port8, Port10, Port11, Port12
4	Port13, Port14, Port15, Port18
5	Port16, Port17, Port19, Port21
6	Port20, Port22, Port23, Port24
7	Port25, Port26, Port27, Port30
8	Port28, Port29, Port31, Port33
9	Port32, Port34, Port35, Port36
10	Port37, Port38, Port39, Port42
11	Port40, Port41, Port43, Port45
12	Port44, Port46, Port47, Port48

When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports of a group can be configured with the same port rate or different rate. When configuring at different port rates, 10G and 1G can coexist, but 25G cannot coexist with 10G or 1G. The following table gives several cases of speed setting for the group of ports.

	Port1	Port2	Port3	Port6	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	×
case #6	25G	10G	25G	10G	×
case #7	25G	1G	10G	25G	×

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
2	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
3	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
4	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
5	te-1/1/5	25Gb/s,10Gb/s,1Gb/s
6	te-1/1/6	25Gb/s,10Gb/s,1Gb/s
7	te-1/1/7	25Gb/s,10Gb/s,1Gb/s
8	te-1/1/8	25Gb/s,10Gb/s,1Gb/s

9	te-1/1/9	25Gb/s,10Gb/s,1Gb/s
10	te-1/1/10	25Gb/s,10Gb/s,1Gb/s
11	te-1/1/11	25Gb/s,10Gb/s,1Gb/s
12	te-1/1/12	25Gb/s,10Gb/s,1Gb/s
13	te-1/1/13	25Gb/s,10Gb/s,1Gb/s
14	te-1/1/14	25Gb/s,10Gb/s,1Gb/s
15	te-1/1/15	25Gb/s,10Gb/s,1Gb/s
16	te-1/1/16	25Gb/s,10Gb/s,1Gb/s
17	te-1/1/17	25Gb/s,10Gb/s,1Gb/s
18	te-1/1/18	25Gb/s,10Gb/s,1Gb/s
19	te-1/1/19	25Gb/s,10Gb/s,1Gb/s
20	te-1/1/20	25Gb/s,10Gb/s,1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s,1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s,1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s,1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s,1Gb/s
25	te-1/1/25	25Gb/s,10Gb/s,1Gb/s
26	te-1/1/26	25Gb/s,10Gb/s,1Gb/s
27	te-1/1/27	25Gb/s,10Gb/s,1Gb/s
28	te-1/1/28	25Gb/s,10Gb/s,1Gb/s
29	te-1/1/29	25Gb/s,10Gb/s,1Gb/s
30	te-1/1/30	25Gb/s,10Gb/s,1Gb/s
31	te-1/1/31	25Gb/s,10Gb/s,1Gb/s
32	te-1/1/32	25Gb/s,10Gb/s,1Gb/s
33	te-1/1/33	25Gb/s,10Gb/s,1Gb/s
34	te-1/1/34	25Gb/s,10Gb/s,1Gb/s
35	te-1/1/35	25Gb/s,10Gb/s,1Gb/s
36	te-1/1/36	25Gb/s,10Gb/s,1Gb/s
37	te-1/1/37	25Gb/s,10Gb/s,1Gb/s
38	te-1/1/38	25Gb/s,10Gb/s,1Gb/s
39	te-1/1/39	25Gb/s,10Gb/s,1Gb/s
40	te-1/1/40	25Gb/s,10Gb/s,1Gb/s
41	te-1/1/41	25Gb/s,10Gb/s,1Gb/s
42	te-1/1/42	25Gb/s,10Gb/s,1Gb/s
43	te-1/1/43	25Gb/s,10Gb/s,1Gb/s
44	te-1/1/44	25Gb/s,10Gb/s,1Gb/s
45	te-1/1/45	25Gb/s,10Gb/s,1Gb/s
46	te-1/1/46	25Gb/s,10Gb/s,1Gb/s
47	te-1/1/47	25Gb/s,10Gb/s,1Gb/s
48	te-1/1/48	25Gb/s,10Gb/s,1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

54	xe-1/1/6	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
55	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
56	xe-1/1/8	100Gb/s,40Gb/s, 4x25Gb/s, 4x10Gb/s
57	me-1/1/1(Management Port)	auto
	te-1/1/49(Front Panel Port)	10Gb/s,1Gb/s
58	me-1/1/2(Management Port)	auto
	te-1/1/50(Front Panel Port)	10Gb/s,1Gb/s

S5810-48TS-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	10/100/1000Mb/s
26	ge-1/1/26	10/100/1000Mb/s
27	ge-1/1/27	10/100/1000Mb/s

28	ge-1/1/28	10/100/1000Mb/s
29	ge-1/1/29	10/100/1000Mb/s
30	ge-1/1/30	10/100/1000Mb/s
31	ge-1/1/31	10/100/1000Mb/s
32	ge-1/1/32	10/100/1000Mb/s
33	ge-1/1/33	10/100/1000Mb/s
34	ge-1/1/34	10/100/1000Mb/s
35	ge-1/1/35	10/100/1000Mb/s
36	ge-1/1/36	10/100/1000Mb/s
37	ge-1/1/37	10/100/1000Mb/s
38	ge-1/1/38	10/100/1000Mb/s
39	ge-1/1/39	10/100/1000Mb/s
40	ge-1/1/40	10/100/1000Mb/s
41	ge-1/1/41	10/100/1000Mb/s
42	ge-1/1/42	10/100/1000Mb/s
43	ge-1/1/43	10/100/1000Mb/s
44	ge-1/1/44	10/100/1000Mb/s
45	ge-1/1/45	10/100/1000Mb/s
46	ge-1/1/46	10/100/1000Mb/s
47	ge-1/1/47	10/100/1000Mb/s
48	ge-1/1/48	10/100/1000Mb/s
49	te-1/1/1	10Gb/s, 1Gb/s
50	te-1/1/2	10Gb/s, 1Gb/s
51	te-1/1/3	10Gb/s, 1Gb/s
52	te-1/1/4	10Gb/s, 1Gb/s

S5810-28FS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
2	ge-1/1/2	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
3	ge-1/1/3	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
4	ge-1/1/4	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
5	ge-1/1/5	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
6	ge-1/1/6	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
7	ge-1/1/7	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
8	ge-1/1/8	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
9	ge-1/1/9	1Gb/s
10	ge-1/1/10	1Gb/s
11	ge-1/1/11	1Gb/s
12	ge-1/1/12	1Gb/s
13	ge-1/1/13	1Gb/s
14	ge-1/1/14	1Gb/s
15	ge-1/1/15	1Gb/s
16	ge-1/1/16	1Gb/s
17	ge-1/1/17	1Gb/s
18	ge-1/1/18	1Gb/s
19	ge-1/1/19	1Gb/s
20	ge-1/1/20	1Gb/s
21	ge-1/1/21	1Gb/s
22	ge-1/1/22	1Gb/s

23	ge-1/1/23	1Gb/s
24	ge-1/1/24	1Gb/s
25	ge-1/1/25	1Gb/s
26	ge-1/1/26	1Gb/s
27	ge-1/1/27	1Gb/s
28	ge-1/1/28	1Gb/s
29	te-1/1/1	10Gb/s, 1Gb/s
30	te-1/1/2	10Gb/s, 1Gb/s
31	te-1/1/3	10Gb/s, 1Gb/s
32	te-1/1/4	10Gb/s, 1Gb/s

S5810-28TS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
26	ge-1/1/26	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)

27	ge-1/1/27	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
28	ge-1/1/28	• 10/100/1000Mb/s (combo port works as RJ45 port) • 1Gb/s (combo port works as GE SFP port)
29	te-1/1/1	10Gb/s, 1Gb/s
30	te-1/1/2	10Gb/s, 1Gb/s
31	te-1/1/3	10Gb/s, 1Gb/s
32	te-1/1/4	10Gb/s, 1Gb/s

S5810-48FS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	1Gb/s
2	ge-1/1/2	1Gb/s
3	ge-1/1/3	1Gb/s
4	ge-1/1/4	1Gb/s
5	ge-1/1/5	1Gb/s
6	ge-1/1/6	1Gb/s
7	ge-1/1/7	1Gb/s
8	ge-1/1/8	1Gb/s
9	ge-1/1/9	1Gb/s
10	ge-1/1/10	1Gb/s
11	ge-1/1/11	1Gb/s
12	ge-1/1/12	1Gb/s
13	ge-1/1/13	1Gb/s
14	ge-1/1/14	1Gb/s
15	ge-1/1/15	1Gb/s
16	ge-1/1/16	1Gb/s
17	ge-1/1/17	1Gb/s
18	ge-1/1/18	1Gb/s
19	ge-1/1/19	1Gb/s
20	ge-1/1/20	1Gb/s
21	ge-1/1/21	1Gb/s
22	ge-1/1/22	1Gb/s
23	ge-1/1/23	1Gb/s
24	ge-1/1/24	1Gb/s
25	ge-1/1/25	1Gb/s
26	ge-1/1/26	1Gb/s
27	ge-1/1/27	1Gb/s

28	ge-1/1/28	1Gb/s
29	ge-1/1/29	1Gb/s
30	ge-1/1/30	1Gb/s
31	ge-1/1/31	1Gb/s
32	ge-1/1/32	1Gb/s
33	ge-1/1/33	1Gb/s
34	ge-1/1/34	1Gb/s
35	ge-1/1/35	1Gb/s
36	ge-1/1/36	1Gb/s
37	ge-1/1/37	1Gb/s
38	ge-1/1/38	1Gb/s
39	ge-1/1/39	1Gb/s
40	ge-1/1/40	1Gb/s
41	ge-1/1/41	1Gb/s
42	ge-1/1/42	1Gb/s
43	ge-1/1/43	1Gb/s
44	ge-1/1/44	1Gb/s
45	ge-1/1/45	1Gb/s
46	ge-1/1/46	1Gb/s
47	ge-1/1/47	1Gb/s
48	ge-1/1/48	1Gb/s
49	te-1/1/1	10Gb/s, 1Gb/s
50	te-1/1/2	10Gb/s, 1Gb/s
51	te-1/1/3	10Gb/s, 1Gb/s
52	te-1/1/4	10Gb/s, 1Gb/s

S5810-48TS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	10/100/1000Mb/s
26	ge-1/1/26	10/100/1000Mb/s
27	ge-1/1/27	10/100/1000Mb/s

28	ge-1/1/28	10/100/1000Mb/s
29	ge-1/1/29	10/100/1000Mb/s
30	ge-1/1/30	10/100/1000Mb/s
31	ge-1/1/31	10/100/1000Mb/s
32	ge-1/1/32	10/100/1000Mb/s
33	ge-1/1/33	10/100/1000Mb/s
34	ge-1/1/34	10/100/1000Mb/s
35	ge-1/1/35	10/100/1000Mb/s
36	ge-1/1/36	10/100/1000Mb/s
37	ge-1/1/37	10/100/1000Mb/s
38	ge-1/1/38	10/100/1000Mb/s
39	ge-1/1/39	10/100/1000Mb/s
40	ge-1/1/40	10/100/1000Mb/s
41	ge-1/1/41	10/100/1000Mb/s
42	ge-1/1/42	10/100/1000Mb/s
43	ge-1/1/43	10/100/1000Mb/s
44	ge-1/1/44	10/100/1000Mb/s
45	ge-1/1/45	10/100/1000Mb/s
46	ge-1/1/46	10/100/1000Mb/s
47	ge-1/1/47	10/100/1000Mb/s
48	ge-1/1/48	10/100/1000Mb/s
49	te-1/1/1	10Gb/s, 1Gb/s
50	te-1/1/2	10Gb/s, 1Gb/s
51	te-1/1/3	10Gb/s, 1Gb/s
52	te-1/1/4	10Gb/s, 1Gb/s

S5860-20SQ Switch Port Name Description

NOTE:

Ports Te-1/1/21, Te-1/1/22, Te-1/1/23 and Te-1/1/24 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/21	te-1/1/22	te-1/1/23	te-1/1/24	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s

14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	25Gb/s,10Gb/s, 1Gb/s
22	te-1/1/22	25Gb/s,10Gb/s, 1Gb/s
23	te-1/1/23	25Gb/s,10Gb/s, 1Gb/s
24	te-1/1/24	25Gb/s,10Gb/s, 1Gb/s
25	xe-1/1/1	40Gb/s, 4 x 10Gb/s, 4 x 1Gb/s
26	xe-1/1/2	40Gb/s, 4 x 10Gb/s, 4 x 1Gb/s

S5860-24XB-U Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	100M/1G/2.5G/5G/10G
2	te-1/1/2	100M/1G/2.5G/5G/10G
3	te-1/1/3	100M/1G/2.5G/5G/10G
4	te-1/1/4	100M/1G/2.5G/5G/10G
5	te-1/1/5	100M/1G/2.5G/5G/10G
6	te-1/1/6	100M/1G/2.5G/5G/10G
7	te-1/1/7	100M/1G/2.5G/5G/10G
8	te-1/1/8	100M/1G/2.5G/5G/10G
9	te-1/1/9	100M/1G/2.5G/5G/10G
10	te-1/1/10	100M/1G/2.5G/5G/10G
11	te-1/1/11	100M/1G/2.5G/5G/10G
12	te-1/1/12	100M/1G/2.5G/5G/10G
13	te-1/1/13	100M/1G/2.5G/5G/10G
14	te-1/1/14	100M/1G/2.5G/5G/10G
15	te-1/1/15	100M/1G/2.5G/5G/10G
16	te-1/1/16	100M/1G/2.5G/5G/10G
17	te-1/1/17	100M/1G/2.5G/5G/10G
18	te-1/1/18	100M/1G/2.5G/5G/10G
19	te-1/1/19	100M/1G/2.5G/5G/10G
20	te-1/1/20	100M/1G/2.5G/5G/10G
21	te-1/1/21	100M/1G/2.5G/5G/10G
22	te-1/1/22	100M/1G/2.5G/5G/10G
23	te-1/1/23	100M/1G/2.5G/5G/10G
24	te-1/1/24	100M/1G/2.5G/5G/10G
25	te-1/1/25	1G/10G
26	te-1/1/26	1G/10G
27	te-1/1/27	1G/10G

28	te-1/1/28	1G/10G
29	te-1/1/29	1G/10G/25G
30	te-1/1/30	1G/10G/25G
31	te-1/1/31	1G/10G/25G
32	te-1/1/32	1G/10G/25G

N8560-32C Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s

28	xe-1/1/28	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s

N8560-64C Switch Port Name Description

Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 2, 3, 9, 10, 17, 18, 19, 25, 26, 27, 33, 34, 41, 42, 49, 50, 57 and 58 can be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s

26	xe-1/1/26	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	xe-1/1/33	100Gb/s, 40Gb/s, 4 x 25Gb/s
34	xe-1/1/34	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
35	xe-1/1/35	100Gb/s, 40Gb/s
36	xe-1/1/36	100Gb/s, 40Gb/s
37	xe-1/1/37	100Gb/s, 40Gb/s
38	xe-1/1/38	100Gb/s, 40Gb/s
39	xe-1/1/39	100Gb/s, 40Gb/s
40	xe-1/1/40	100Gb/s, 40Gb/s
41	xe-1/1/41	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
42	xe-1/1/42	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
43	xe-1/1/43	100Gb/s, 40Gb/s
44	xe-1/1/44	100Gb/s, 40Gb/s
45	xe-1/1/45	100Gb/s, 40Gb/s
46	xe-1/1/46	100Gb/s, 40Gb/s
47	xe-1/1/47	100Gb/s, 40Gb/s
48	xe-1/1/48	100Gb/s, 40Gb/s
49	xe-1/1/49	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
50	xe-1/1/50	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
51	xe-1/1/51	100Gb/s, 40Gb/s
52	xe-1/1/52	100Gb/s, 40Gb/s
53	xe-1/1/53	100Gb/s, 40Gb/s
54	xe-1/1/54	100Gb/s, 40Gb/s
55	xe-1/1/55	100Gb/s, 40Gb/s
56	xe-1/1/56	100Gb/s, 40Gb/s
57	xe-1/1/57	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s

58	xe-1/1/58	100Gb/s, 40Gb/s, 4 x 25Gb/s, 4 x 10Gb/s
59	xe-1/1/59	100Gb/s, 40Gb/s
60	xe-1/1/60	100Gb/s, 40Gb/s
61	xe-1/1/61	100Gb/s, 40Gb/s
62	xe-1/1/62	100Gb/s, 40Gb/s
63	xe-1/1/63	100Gb/s, 40Gb/s
64	xe-1/1/64	100Gb/s, 40Gb/s

S5860-24MG-U Switch Port Name Description

NOTE:

Ports te-1/1/1, te-1/1/2, te-1/1/3 and te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with 10G or 1G. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	×
case #6	25G	10G	25G	10G	×
case #7	25G	1G	10G	25G	×

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	100M/1G/2.5G/5G
2	ge-1/1/2	100M/1G/2.5G/5G
3	ge-1/1/3	100M/1G/2.5G/5G
4	ge-1/1/4	100M/1G/2.5G/5G
5	ge-1/1/5	100M/1G/2.5G/5G
6	ge-1/1/6	100M/1G/2.5G/5G
7	ge-1/1/7	100M/1G/2.5G/5G
8	ge-1/1/8	100M/1G/2.5G/5G
9	ge-1/1/9	100M/1G/2.5G/5G
10	ge-1/1/10	100M/1G/2.5G/5G
11	ge-1/1/11	100M/1G/2.5G/5G
12	ge-1/1/12	100M/1G/2.5G/5G
13	ge-1/1/13	100M/1G/2.5G/5G

14	ge-1/1/14	100M/1G/2.5G/5G
15	ge-1/1/15	100M/1G/2.5G/5G
16	ge-1/1/16	100M/1G/2.5G/5G
17	ge-1/1/17	100M/1G/2.5G/5G
18	ge-1/1/18	100M/1G/2.5G/5G
19	ge-1/1/19	100M/1G/2.5G/5G
20	ge-1/1/20	100M/1G/2.5G/5G
21	ge-1/1/21	100M/1G/2.5G/5G
22	ge-1/1/22	100M/1G/2.5G/5G
23	ge-1/1/23	100M/1G/2.5G/5G
24	ge-1/1/24	100M/1G/2.5G/5G
25	te-1/1/1	1G/10G/25G
26	te-1/1/2	1G/10G/25G
27	te-1/1/3	1G/10G/25G
28	te-1/1/4	1G/10G/25G

S5860-48XMG-U/S5860-48XMG Switch Port Name Description

NOTE:
Ports te-1/1/49, te-1/1/50, te-1/1/51 and te-1/1/52 are a group of SFP28 25G ports which don't support to configure the port rate to 10 Gbit/s or 1 Gbit/s.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
2	te-1/1/2	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
3	te-1/1/3	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
4	te-1/1/4	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
5	te-1/1/5	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
6	te-1/1/6	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
7	te-1/1/7	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
8	te-1/1/8	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
9	te-1/1/9	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
10	te-1/1/10	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
11	te-1/1/11	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
12	te-1/1/12	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
13	te-1/1/13	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
14	te-1/1/14	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
15	te-1/1/15	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
16	te-1/1/16	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
17	te-1/1/17	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
18	te-1/1/18	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
19	te-1/1/19	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
20	te-1/1/20	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
21	te-1/1/21	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
22	te-1/1/22	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
23	te-1/1/23	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
24	te-1/1/24	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s

25	te-1/1/25	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
26	te-1/1/26	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
27	te-1/1/27	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
28	te-1/1/28	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
29	te-1/1/29	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
30	te-1/1/30	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
31	te-1/1/31	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
32	te-1/1/32	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
33	te-1/1/33	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
34	te-1/1/34	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
35	te-1/1/35	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
36	te-1/1/36	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
37	te-1/1/37	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
38	te-1/1/38	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
39	te-1/1/39	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
40	te-1/1/40	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
41	te-1/1/41	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
42	te-1/1/42	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
43	te-1/1/43	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
44	te-1/1/44	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
45	te-1/1/45	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
46	te-1/1/46	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
47	te-1/1/47	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
48	te-1/1/48	10Gb/s, 5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/49	25Gb/s
50	te-1/1/50	25Gb/s
51	te-1/1/51	25Gb/s
52	te-1/1/52	25Gb/s
53	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s

S5860-24XMG Switch Port Name Description

NOTE:

Ports te-1/1/29, te-1/1/30, te-1/1/31 and te-1/1/32 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with 10G or 1G. The following table gives several cases of speed setting for this group of ports.

	te-1/1/29	te-1/1/30	te-1/1/31	te-1/1/32	Allowed or not allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	×
case #6	25G	10G	25G	10G	×
case #7	25G	1G	10G	25G	×

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	100M/1G/2.5G/5G/10G
2	te-1/1/2	100M/1G/2.5G/5G/10G
3	te-1/1/3	100M/1G/2.5G/5G/10G
4	te-1/1/4	100M/1G/2.5G/5G/10G
5	te-1/1/5	100M/1G/2.5G/5G/10G
6	te-1/1/6	100M/1G/2.5G/5G/10G
7	te-1/1/7	100M/1G/2.5G/5G/10G
8	te-1/1/8	100M/1G/2.5G/5G/10G
9	te-1/1/9	100M/1G/2.5G/5G/10G
10	te-1/1/10	100M/1G/2.5G/5G/10G
11	te-1/1/11	100M/1G/2.5G/5G/10G
12	te-1/1/12	100M/1G/2.5G/5G/10G
13	te-1/1/13	100M/1G/2.5G/5G/10G

14	te-1/1/14	100M/1G/2.5G/5G/10G
15	te-1/1/15	100M/1G/2.5G/5G/10G
16	te-1/1/16	100M/1G/2.5G/5G/10G
17	te-1/1/17	100M/1G/2.5G/5G/10G
18	te-1/1/18	100M/1G/2.5G/5G/10G
19	te-1/1/19	100M/1G/2.5G/5G/10G
20	te-1/1/20	100M/1G/2.5G/5G/10G
21	te-1/1/21	100M/1G/2.5G/5G/10G
22	te-1/1/22	100M/1G/2.5G/5G/10G
23	te-1/1/23	100M/1G/2.5G/5G/10G
24	te-1/1/24	100M/1G/2.5G/5G/10G
25	te-1/1/25	1G/10G
26	te-1/1/26	1G/10G
27	te-1/1/27	1G/10G
28	te-1/1/28	1G/10G
29	te-1/1/29	1G/10G/25G
30	te-1/1/30	1G/10G/25G
31	te-1/1/31	1G/10G/25G
32	te-1/1/32	1G/10G/25G

S5860-48MG-U Switch Port Name Description

NOTE:

Ports te-1/1/49, te-1/1/50, te-1/1/51 and te-1/1/52 are a group of SFP28 25G ports which don't support to configure the port rate to 10 Gbit/s or 1 Gbit/s.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
2	ge-1/1/2	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
3	ge-1/1/3	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
4	ge-1/1/4	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
5	ge-1/1/5	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
6	ge-1/1/6	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
7	ge-1/1/7	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
8	ge-1/1/8	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
9	ge-1/1/9	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
10	ge-1/1/10	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
11	ge-1/1/11	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
12	ge-1/1/12	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
13	ge-1/1/13	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
14	ge-1/1/14	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
15	ge-1/1/15	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
16	ge-1/1/16	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
17	ge-1/1/17	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
18	ge-1/1/18	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
19	ge-1/1/19	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
20	ge-1/1/20	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
21	ge-1/1/21	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
22	ge-1/1/22	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
23	ge-1/1/23	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
24	ge-1/1/24	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s

25	ge-1/1/25	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
26	ge-1/1/26	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
27	ge-1/1/27	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
28	ge-1/1/28	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
29	ge-1/1/29	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
30	ge-1/1/30	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
31	ge-1/1/31	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
32	ge-1/1/32	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
33	ge-1/1/33	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
34	ge-1/1/34	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
35	ge-1/1/35	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
36	ge-1/1/36	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
37	ge-1/1/37	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
38	ge-1/1/38	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
39	ge-1/1/39	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
40	ge-1/1/40	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
41	ge-1/1/41	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
42	ge-1/1/42	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
43	ge-1/1/43	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
44	ge-1/1/44	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
45	ge-1/1/45	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
46	ge-1/1/46	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
47	ge-1/1/47	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
48	ge-1/1/48	5Gb/s, 2.5Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/1	25G
50	te-1/1/2	25G
51	te-1/1/3	25G
52	te-1/1/4	25G
53	xe-1/1/1	40Gb/s, 4x10Gb/s, 4x1Gb/s
54	xe-1/1/2	40Gb/s, 4x10Gb/s, 4x1Gb/s

S5870-48T6S-U/S5870-48T6S Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	10/100/1000M
2	ge-1/1/2	10/100/1000M
3	ge-1/1/3	10/100/1000M
4	ge-1/1/4	10/100/1000M
5	ge-1/1/5	10/100/1000M
6	ge-1/1/6	10/100/1000M
7	ge-1/1/7	10/100/1000M
8	ge-1/1/8	10/100/1000M
9	ge-1/1/9	10/100/1000M
10	ge-1/1/10	10/100/1000M
11	ge-1/1/11	10/100/1000M
12	ge-1/1/12	10/100/1000M
13	ge-1/1/13	10/100/1000M
14	ge-1/1/14	10/100/1000M
15	ge-1/1/15	10/100/1000M
16	ge-1/1/16	10/100/1000M
17	ge-1/1/17	10/100/1000M
18	ge-1/1/18	10/100/1000M
19	ge-1/1/19	10/100/1000M
20	ge-1/1/20	10/100/1000M
21	ge-1/1/21	10/100/1000M
22	ge-1/1/22	10/100/1000M
23	ge-1/1/23	10/100/1000M
24	ge-1/1/24	10/100/1000M
25	ge-1/1/25	10/100/1000M
26	ge-1/1/26	10/100/1000M
27	ge-1/1/27	10/100/1000M
28	ge-1/1/28	10/100/1000M
29	ge-1/1/29	10/100/1000M
30	ge-1/1/30	10/100/1000M
31	ge-1/1/31	10/100/1000M
32	ge-1/1/32	10/100/1000M
33	ge-1/1/33	10/100/1000M
34	ge-1/1/34	10/100/1000M
35	ge-1/1/35	10/100/1000M
36	ge-1/1/36	10/100/1000M
37	ge-1/1/37	10/100/1000M
38	ge-1/1/38	10/100/1000M
39	ge-1/1/39	10/100/1000M

40	ge-1/1/40	10/100/1000M
41	ge-1/1/41	10/100/1000M
42	ge-1/1/42	10/100/1000M
43	ge-1/1/43	10/100/1000M
44	ge-1/1/44	10/100/1000M
45	ge-1/1/45	10/100/1000M
46	ge-1/1/46	10/100/1000M
47	ge-1/1/47	10/100/1000M
48	ge-1/1/48	10/100/1000M
49	te-1/1/1	10G, 1G
50	te-1/1/2	10G, 1G
51	te-1/1/3	10G, 1G
52	te-1/1/4	10G, 1G
53	te-1/1/5	10G, 1G
54	te-1/1/6	10G, 1G

S5870-48T6BC/S5870-48T6BC-U Switch Port Name Description

NOTE:
Ports Te-1/1/1, Te-1/1/2, Te-1/1/3 and Te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not Allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note: If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	1Gb/s, 100Mb/s, 10Mb/s
2	ge-1/1/2	1Gb/s, 100Mb/s, 10Mb/s
3	ge-1/1/3	1Gb/s, 100Mb/s, 10Mb/s
4	ge-1/1/4	1Gb/s, 100Mb/s, 10Mb/s
5	ge-1/1/5	1Gb/s, 100Mb/s, 10Mb/s
6	ge-1/1/6	1Gb/s, 100Mb/s, 10Mb/s
7	ge-1/1/7	1Gb/s, 100Mb/s, 10Mb/s
8	ge-1/1/8	1Gb/s, 100Mb/s, 10Mb/s
9	ge-1/1/9	1Gb/s, 100Mb/s, 10Mb/s
10	ge-1/1/10	1Gb/s, 100Mb/s, 10Mb/s
11	ge-1/1/11	1Gb/s, 100Mb/s, 10Mb/s
12	ge-1/1/12	1Gb/s, 100Mb/s, 10Mb/s
13	ge-1/1/13	1Gb/s, 100Mb/s, 10Mb/s
14	ge-1/1/14	1Gb/s, 100Mb/s, 10Mb/s
15	ge-1/1/15	1Gb/s, 100Mb/s, 10Mb/s
16	ge-1/1/16	1Gb/s, 100Mb/s, 10Mb/s
17	ge-1/1/17	1Gb/s, 100Mb/s, 10Mb/s
18	ge-1/1/18	1Gb/s, 100Mb/s, 10Mb/s
19	ge-1/1/19	1Gb/s, 100Mb/s, 10Mb/s
20	ge-1/1/20	1Gb/s, 100Mb/s, 10Mb/s
21	ge-1/1/21	1Gb/s, 100Mb/s, 10Mb/s
22	ge-1/1/22	1Gb/s, 100Mb/s, 10Mb/s
23	ge-1/1/23	1Gb/s, 100Mb/s, 10Mb/s
24	ge-1/1/24	1Gb/s, 100Mb/s, 10Mb/s
25	ge-1/1/25	1Gb/s, 100Mb/s, 10Mb/s
26	ge-1/1/26	1Gb/s, 100Mb/s, 10Mb/s

Physical Port Number	Interface Names	Interface Supported Speed
27	ge-1/1/27	1Gb/s, 100Mb/s, 10Mb/s
28	ge-1/1/28	1Gb/s, 100Mb/s, 10Mb/s
29	ge-1/1/29	1Gb/s, 100Mb/s, 10Mb/s
30	ge-1/1/30	1Gb/s, 100Mb/s, 10Mb/s
31	ge-1/1/31	1Gb/s, 100Mb/s, 10Mb/s
32	ge-1/1/32	1Gb/s, 100Mb/s, 10Mb/s
33	ge-1/1/33	1Gb/s, 100Mb/s, 10Mb/s
34	ge-1/1/34	1Gb/s, 100Mb/s, 10Mb/s
35	ge-1/1/35	1Gb/s, 100Mb/s, 10Mb/s
36	ge-1/1/36	1Gb/s, 100Mb/s, 10Mb/s
37	ge-1/1/37	1Gb/s, 100Mb/s, 10Mb/s
38	ge-1/1/38	1Gb/s, 100Mb/s, 10Mb/s
39	ge-1/1/39	1Gb/s, 100Mb/s, 10Mb/s
40	ge-1/1/40	1Gb/s, 100Mb/s, 10Mb/s
41	ge-1/1/41	1Gb/s, 100Mb/s, 10Mb/s
42	ge-1/1/42	1Gb/s, 100Mb/s, 10Mb/s
43	ge-1/1/43	1Gb/s, 100Mb/s, 10Mb/s
44	ge-1/1/44	1Gb/s, 100Mb/s, 10Mb/s
45	ge-1/1/45	1Gb/s, 100Mb/s, 10Mb/s
46	ge-1/1/46	1Gb/s, 100Mb/s, 10Mb/s
47	ge-1/1/47	1Gb/s, 100Mb/s, 10Mb/s
48	ge-1/1/48	1Gb/s, 100Mb/s, 10Mb/s
49	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

N5850-48X6C Switch Port Name Description

NOTE:

Due to hardware limitations, only ports xe-1/1/1 and xe-1/1/4 support to be split into four Gigabit Ethernet interfaces, other ports are not supported to be split.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s

25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s
27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s

N8550-64C Switch Port Name Description

NOTE:
Only the ports on the first row of front panel are allowed to do breakout, that is, only ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 and 31 can be split into four Gigabit Ethernet interfaces.

Mapping between physical ports, interface names and interface supported speed on N8550-64C are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
2	xe-1/1/2	100Gb/s, 40Gb/s
3	xe-1/1/3	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
4	xe-1/1/4	100Gb/s, 40Gb/s
5	xe-1/1/5	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
6	xe-1/1/6	100Gb/s, 40Gb/s
7	xe-1/1/7	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
8	xe-1/1/8	100Gb/s, 40Gb/s
9	xe-1/1/9	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
10	xe-1/1/10	100Gb/s, 40Gb/s
11	xe-1/1/11	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
12	xe-1/1/12	100Gb/s, 40Gb/s
13	xe-1/1/13	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
14	xe-1/1/14	100Gb/s, 40Gb/s
15	xe-1/1/15	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
16	xe-1/1/16	100Gb/s, 40Gb/s
17	xe-1/1/17	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
18	xe-1/1/18	100Gb/s, 40Gb/s
19	xe-1/1/19	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
20	xe-1/1/20	100Gb/s, 40Gb/s
21	xe-1/1/21	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
22	xe-1/1/22	100Gb/s, 40Gb/s
23	xe-1/1/23	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
24	xe-1/1/24	100Gb/s, 40Gb/s
25	xe-1/1/25	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
26	xe-1/1/26	100Gb/s, 40Gb/s
27	xe-1/1/27	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
28	xe-1/1/28	100Gb/s, 40Gb/s
29	xe-1/1/29	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
30	xe-1/1/30	100Gb/s, 40Gb/s
31	xe-1/1/31	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
32	xe-1/1/32	100Gb/s, 40Gb/s
33	xe-1/1/33	100Gb/s, 40Gb/s
34	xe-1/1/34	100Gb/s, 40Gb/s
35	xe-1/1/35	100Gb/s, 40Gb/s
36	xe-1/1/36	100Gb/s, 40Gb/s

37	xe-1/1/37	100Gb/s, 40Gb/s
38	xe-1/1/38	100Gb/s, 40Gb/s
39	xe-1/1/39	100Gb/s, 40Gb/s
40	xe-1/1/40	100Gb/s, 40Gb/s
41	xe-1/1/41	100Gb/s, 40Gb/s
42	xe-1/1/42	100Gb/s, 40Gb/s
43	xe-1/1/43	100Gb/s, 40Gb/s
44	xe-1/1/44	100Gb/s, 40Gb/s
45	xe-1/1/45	100Gb/s, 40Gb/s
46	xe-1/1/46	100Gb/s, 40Gb/s
47	xe-1/1/47	100Gb/s, 40Gb/s
48	xe-1/1/48	100Gb/s, 40Gb/s
49	xe-1/1/49	100Gb/s, 40Gb/s
50	xe-1/1/50	100Gb/s, 40Gb/s
51	xe-1/1/51	100Gb/s, 40Gb/s
52	xe-1/1/52	100Gb/s, 40Gb/s
53	xe-1/1/53	100Gb/s, 40Gb/s
54	xe-1/1/54	100Gb/s, 40Gb/s
55	xe-1/1/55	100Gb/s, 40Gb/s
56	xe-1/1/56	100Gb/s, 40Gb/s
57	xe-1/1/57	100Gb/s, 40Gb/s
58	xe-1/1/58	100Gb/s, 40Gb/s
59	xe-1/1/59	100Gb/s, 40Gb/s
60	xe-1/1/60	100Gb/s, 40Gb/s
61	xe-1/1/61	100Gb/s, 40Gb/s
62	xe-1/1/62	100Gb/s, 40Gb/s
63	xe-1/1/63	100Gb/s, 40Gb/s
64	xe-1/1/64	100Gb/s, 40Gb/s

N9550-32D Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
2	xe-1/1/2	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
3	xe-1/1/3	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
4	xe-1/1/4	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
5	xe-1/1/5	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
6	xe-1/1/6	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
7	xe-1/1/7	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
8	xe-1/1/8	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
9	xe-1/1/9	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
10	xe-1/1/10	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
11	xe-1/1/11	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
12	xe-1/1/12	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
13	xe-1/1/13	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
14	xe-1/1/14	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
15	xe-1/1/15	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
16	xe-1/1/16	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
17	xe-1/1/17	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s

18	xe-1/1/18	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
19	xe-1/1/19	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
20	xe-1/1/20	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
21	xe-1/1/21	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
22	xe-1/1/22	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
23	xe-1/1/23	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
24	xe-1/1/24	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
25	xe-1/1/25	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
26	xe-1/1/26	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
27	xe-1/1/27	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
28	xe-1/1/28	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
29	xe-1/1/29	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
30	xe-1/1/30	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
31	xe-1/1/31	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s
32	xe-1/1/32	400Gb/s, 100Gb/s, 4 x 100Gb/s，2 x 200Gb/s

N5850-48S6C Switch Port Name Description

NOTE:

Due to hardware limitations, only ports xe-1/1/1 and xe-1/1/4 support to be split into four Gigabit Ethernet interfaces, other ports are not supported to be split.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	te-1/1/1	10Gb/s, 1Gb/s
2	te-1/1/2	10Gb/s, 1Gb/s
3	te-1/1/3	10Gb/s, 1Gb/s
4	te-1/1/4	10Gb/s, 1Gb/s
5	te-1/1/5	10Gb/s, 1Gb/s
6	te-1/1/6	10Gb/s, 1Gb/s
7	te-1/1/7	10Gb/s, 1Gb/s
8	te-1/1/8	10Gb/s, 1Gb/s
9	te-1/1/9	10Gb/s, 1Gb/s
10	te-1/1/10	10Gb/s, 1Gb/s
11	te-1/1/11	10Gb/s, 1Gb/s
12	te-1/1/12	10Gb/s, 1Gb/s
13	te-1/1/13	10Gb/s, 1Gb/s
14	te-1/1/14	10Gb/s, 1Gb/s
15	te-1/1/15	10Gb/s, 1Gb/s
16	te-1/1/16	10Gb/s, 1Gb/s
17	te-1/1/17	10Gb/s, 1Gb/s
18	te-1/1/18	10Gb/s, 1Gb/s
19	te-1/1/19	10Gb/s, 1Gb/s
20	te-1/1/20	10Gb/s, 1Gb/s
21	te-1/1/21	10Gb/s, 1Gb/s
22	te-1/1/22	10Gb/s, 1Gb/s
23	te-1/1/23	10Gb/s, 1Gb/s
24	te-1/1/24	10Gb/s, 1Gb/s

25	te-1/1/25	10Gb/s, 1Gb/s
26	te-1/1/26	10Gb/s, 1Gb/s
27	te-1/1/27	10Gb/s, 1Gb/s
28	te-1/1/28	10Gb/s, 1Gb/s
29	te-1/1/29	10Gb/s, 1Gb/s
30	te-1/1/30	10Gb/s, 1Gb/s
31	te-1/1/31	10Gb/s, 1Gb/s
32	te-1/1/32	10Gb/s, 1Gb/s
33	te-1/1/33	10Gb/s, 1Gb/s
34	te-1/1/34	10Gb/s, 1Gb/s
35	te-1/1/35	10Gb/s, 1Gb/s
36	te-1/1/36	10Gb/s, 1Gb/s
37	te-1/1/37	10Gb/s, 1Gb/s
38	te-1/1/38	10Gb/s, 1Gb/s
39	te-1/1/39	10Gb/s, 1Gb/s
40	te-1/1/40	10Gb/s, 1Gb/s
41	te-1/1/41	10Gb/s, 1Gb/s
42	te-1/1/42	10Gb/s, 1Gb/s
43	te-1/1/43	10Gb/s, 1Gb/s
44	te-1/1/44	10Gb/s, 1Gb/s
45	te-1/1/45	10Gb/s, 1Gb/s
46	te-1/1/46	10Gb/s, 1Gb/s
47	te-1/1/47	10Gb/s, 1Gb/s
48	te-1/1/48	10Gb/s, 1Gb/s
49	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
50	xe-1/1/2	100Gb/s, 40Gb/s
51	xe-1/1/3	100Gb/s, 40Gb/s
52	xe-1/1/4	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
53	xe-1/1/5	100Gb/s, 40Gb/s
54	xe-1/1/6	100Gb/s, 40Gb/s

S5870-48MX6BC-U Switch Port Name Description

NOTE:
Ports Te-1/1/1, Te-1/1/2, Te-1/1/3 and Te-1/1/4 are a group of ports, you should manually configure the port speed for these four ports by using the **set interface gigabit-ethernet speed** command before inserting an optical module. When configuring the rate, the supported port rates are 25 Gbit/s, 10 Gbit/s, and 1 Gbit/s. The four ports can be configured with the same port rate or different rate. When configured at different port rates, 10G and 1G can coexist, but 25G cannot coexist with other rates. The following table gives several cases of speed setting for this group of ports.

	te-1/1/1	te-1/1/2	te-1/1/3	te-1/1/4	Allowed or not Allowed
case #1	10 G	10G	10G	10G	✓
case #2	1G	1G	1G	1G	✓
case #3	25G	25G	25G	25G	✓
case #4	1G	10G	1G	10G	✓
case #5	25G	1G	25G	25G	**X**
case #6	25G	10G	25G	10G	**X**
case #7	25G	1G	10G	25G	**X**

Note: If the port rate is set to 25 Gbit/s, but a 10 Gbit/s optical module is inserted, the port cannot go up.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Supported Speed
1	ge-1/1/1	2.5 Gb/s, 1 Gb/s, 100Mb/s
2	ge-1/1/2	2.5 Gb/s, 1 Gb/s, 100Mb/s
3	ge-1/1/3	2.5 Gb/s, 1 Gb/s, 100Mb/s
4	ge-1/1/4	2.5 Gb/s, 1 Gb/s, 100Mb/s
5	ge-1/1/5	2.5 Gb/s, 1 Gb/s, 100Mb/s
6	ge-1/1/6	2.5 Gb/s, 1 Gb/s, 100Mb/s
7	ge-1/1/7	2.5 Gb/s, 1 Gb/s, 100Mb/s
8	ge-1/1/8	2.5 Gb/s, 1 Gb/s, 100Mb/s
9	ge-1/1/9	2.5 Gb/s, 1 Gb/s, 100Mb/s
10	ge-1/1/10	2.5 Gb/s, 1 Gb/s, 100Mb/s
11	ge-1/1/11	2.5 Gb/s, 1 Gb/s, 100Mb/s
12	ge-1/1/12	2.5 Gb/s, 1 Gb/s, 100Mb/s
13	ge-1/1/13	2.5 Gb/s, 1 Gb/s, 100Mb/s
14	ge-1/1/14	2.5 Gb/s, 1 Gb/s, 100Mb/s
15	ge-1/1/15	2.5 Gb/s, 1 Gb/s, 100Mb/s
16	ge-1/1/16	2.5 Gb/s, 1 Gb/s, 100Mb/s
17	ge-1/1/17	2.5 Gb/s, 1 Gb/s, 100Mb/s
18	ge-1/1/18	2.5 Gb/s, 1 Gb/s, 100Mb/s
19	ge-1/1/19	2.5 Gb/s, 1 Gb/s, 100Mb/s
20	ge-1/1/20	2.5 Gb/s, 1 Gb/s, 100Mb/s
21	ge-1/1/21	2.5 Gb/s, 1 Gb/s, 100Mb/s
22	ge-1/1/22	2.5 Gb/s, 1 Gb/s, 100Mb/s
23	ge-1/1/23	2.5 Gb/s, 1 Gb/s, 100Mb/s
24	ge-1/1/24	2.5 Gb/s, 1 Gb/s, 100Mb/s
25	ge-1/1/25	2.5 Gb/s, 1 Gb/s, 100Mb/s
26	ge-1/1/26	2.5 Gb/s, 1 Gb/s, 100Mb/s

27	ge-1/1/27	2.5 Gb/s, 1 Gb/s, 100Mb/s
28	ge-1/1/28	2.5 Gb/s, 1 Gb/s, 100Mb/s
29	ge-1/1/29	2.5 Gb/s, 1 Gb/s, 100Mb/s
30	ge-1/1/30	2.5 Gb/s, 1 Gb/s, 100Mb/s
31	ge-1/1/31	2.5 Gb/s, 1 Gb/s, 100Mb/s
32	ge-1/1/32	2.5 Gb/s, 1 Gb/s, 100Mb/s
33	ge-1/1/33	2.5 Gb/s, 1 Gb/s, 100Mb/s
34	ge-1/1/34	2.5 Gb/s, 1 Gb/s, 100Mb/s
35	ge-1/1/35	2.5 Gb/s, 1 Gb/s, 100Mb/s
36	ge-1/1/36	2.5 Gb/s, 1 Gb/s, 100Mb/s
37	ge-1/1/37	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
38	ge-1/1/38	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
39	ge-1/1/39	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
40	ge-1/1/40	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
41	ge-1/1/41	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
42	ge-1/1/42	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
43	ge-1/1/43	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
44	ge-1/1/44	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
45	ge-1/1/45	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
46	ge-1/1/46	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
47	ge-1/1/47	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
48	ge-1/1/48	10Gb/s, 5 Gb/s, 2.5 Gb/s, 1Gb/s, 100Mb/s
49	te-1/1/1	25Gb/s,10Gb/s,1Gb/s
50	te-1/1/2	25Gb/s,10Gb/s,1Gb/s
51	te-1/1/3	25Gb/s,10Gb/s,1Gb/s
52	te-1/1/4	25Gb/s,10Gb/s,1Gb/s
53	xe-1/1/1	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s
54	xe-1/1/2	100Gb/s, 40Gb/s, 4x25Gb/s, 4x10Gb/s

S3410-24TS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	te-1/1/1	10Gb/s, 1Gb/s
26	te-1/1/2	10Gb/s, 1Gb/s
27	te-1/1/3	10Gb/s, 1Gb/s

28	te-1/1/4	10Gb/s, 1Gb/s

S3410L-24TF Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	te-1/1/1	1Gb/s
26	te-1/1/2	1Gb/s
27	te-1/1/3	1Gb/s

28	te-1/1/4	1Gb/s

S3410L-24TF-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	te-1/1/1	1Gb/s
26	te-1/1/2	1Gb/s
27	te-1/1/3	1Gb/s

28	te-1/1/4	1Gb/s

S3410-24TS-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	te-1/1/1	10Gb/s, 1Gb/s
26	te-1/1/2	10Gb/s, 1Gb/s

S3410C-16TMS-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	1000Mb/2.5Gb/5Gb/s
2	ge-1/1/2	1000Mb/2.5Gb/5Gb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/15	10/100/1000Mb/s
18	ge-1/1/16	10/100/1000Mb/s
19	te-1/1/1	1/10Gb/s
20	te-1/1/2	1/10Gb/s

S3410C-16TF-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	te-1/1/1	1Gb/s
18	te-1/1/2	1Gb/s

S3410C-8TMS-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	1/2.5/5Gb/s
2	ge-1/1/2	1/2.5/5Gb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	te-1/1/1	1/10Gb/s
12	te-1/1/2	1/10Gb/s

S3410C-16TF Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	te-1/1/1	1Gb/s
18	te-1/1/2	1Gb/s

S3410-48TS-P Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	10/100/1000Mb/s
26	ge-1/1/26	10/100/1000Mb/s
27	ge-1/1/27	10/100/1000Mb/s

28	ge-1/1/28	10/100/1000Mb/s
29	ge-1/1/29	10/100/1000Mb/s
30	ge-1/1/30	10/100/1000Mb/s
31	ge-1/1/31	10/100/1000Mb/s
32	ge-1/1/32	10/100/1000Mb/s
33	ge-1/1/33	10/100/1000Mb/s
34	ge-1/1/34	10/100/1000Mb/s
35	ge-1/1/35	10/100/1000Mb/s
36	ge-1/1/36	10/100/1000Mb/s
37	ge-1/1/37	10/100/1000Mb/s
38	ge-1/1/38	10/100/1000Mb/s
39	ge-1/1/39	10/100/1000Mb/s
40	ge-1/1/40	10/100/1000Mb/s
41	ge-1/1/41	10/100/1000Mb/s
42	ge-1/1/42	10/100/1000Mb/s
43	ge-1/1/43	10/100/1000Mb/s
44	ge-1/1/44	10/100/1000Mb/s
45	ge-1/1/45	10/100/1000Mb/s
46	ge-1/1/46	10/100/1000Mb/s
47	ge-1/1/47	10/100/1000Mb/s
48	ge-1/1/48	10/100/1000Mb/s
49	te-1/1/1	10Gb/s, 1Gb/s
50	te-1/1/2	10Gb/s, 1Gb/s

S3410-48TS Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	10/100/1000Mb/s
26	ge-1/1/26	10/100/1000Mb/s
27	ge-1/1/27	10/100/1000Mb/s

28	ge-1/1/28	10/100/1000Mb/s
29	ge-1/1/29	10/100/1000Mb/s
30	ge-1/1/30	10/100/1000Mb/s
31	ge-1/1/31	10/100/1000Mb/s
32	ge-1/1/32	10/100/1000Mb/s
33	ge-1/1/33	10/100/1000Mb/s
34	ge-1/1/34	10/100/1000Mb/s
35	ge-1/1/35	10/100/1000Mb/s
36	ge-1/1/36	10/100/1000Mb/s
37	ge-1/1/37	10/100/1000Mb/s
38	ge-1/1/38	10/100/1000Mb/s
39	ge-1/1/39	10/100/1000Mb/s
40	ge-1/1/40	10/100/1000Mb/s
41	ge-1/1/41	10/100/1000Mb/s
42	ge-1/1/42	10/100/1000Mb/s
43	ge-1/1/43	10/100/1000Mb/s
44	ge-1/1/44	10/100/1000Mb/s
45	ge-1/1/45	10/100/1000Mb/s
46	ge-1/1/46	10/100/1000Mb/s
47	ge-1/1/47	10/100/1000Mb/s
48	ge-1/1/48	10/100/1000Mb/s
49	te-1/1/1	10Gb/s
50	te-1/1/2	10Gb/s
51	te-1/1/3	10Gb/s
52	te-1/1/4	10Gb/s

S3410L-48TF Switch Port Name Description

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	ge-1/1/1	10/100/1000Mb/s
2	ge-1/1/2	10/100/1000Mb/s
3	ge-1/1/3	10/100/1000Mb/s
4	ge-1/1/4	10/100/1000Mb/s
5	ge-1/1/5	10/100/1000Mb/s
6	ge-1/1/6	10/100/1000Mb/s
7	ge-1/1/7	10/100/1000Mb/s
8	ge-1/1/8	10/100/1000Mb/s
9	ge-1/1/9	10/100/1000Mb/s
10	ge-1/1/10	10/100/1000Mb/s
11	ge-1/1/11	10/100/1000Mb/s
12	ge-1/1/12	10/100/1000Mb/s
13	ge-1/1/13	10/100/1000Mb/s
14	ge-1/1/14	10/100/1000Mb/s
15	ge-1/1/15	10/100/1000Mb/s
16	ge-1/1/16	10/100/1000Mb/s
17	ge-1/1/17	10/100/1000Mb/s
18	ge-1/1/18	10/100/1000Mb/s
19	ge-1/1/19	10/100/1000Mb/s
20	ge-1/1/20	10/100/1000Mb/s
21	ge-1/1/21	10/100/1000Mb/s
22	ge-1/1/22	10/100/1000Mb/s
23	ge-1/1/23	10/100/1000Mb/s
24	ge-1/1/24	10/100/1000Mb/s
25	ge-1/1/25	10/100/1000Mb/s
26	ge-1/1/26	10/100/1000Mb/s
27	ge-1/1/27	10/100/1000Mb/s

28	ge-1/1/28	10/100/1000Mb/s
29	ge-1/1/29	10/100/1000Mb/s
30	ge-1/1/30	10/100/1000Mb/s
31	ge-1/1/31	10/100/1000Mb/s
32	ge-1/1/32	10/100/1000Mb/s
33	ge-1/1/33	10/100/1000Mb/s
34	ge-1/1/34	10/100/1000Mb/s
35	ge-1/1/35	10/100/1000Mb/s
36	ge-1/1/36	10/100/1000Mb/s
37	ge-1/1/37	10/100/1000Mb/s
38	ge-1/1/38	10/100/1000Mb/s
39	ge-1/1/39	10/100/1000Mb/s
40	ge-1/1/40	10/100/1000Mb/s
41	ge-1/1/41	10/100/1000Mb/s
42	ge-1/1/42	10/100/1000Mb/s
43	ge-1/1/43	10/100/1000Mb/s
44	ge-1/1/44	10/100/1000Mb/s
45	ge-1/1/45	10/100/1000Mb/s
46	ge-1/1/46	10/100/1000Mb/s
47	ge-1/1/47	10/100/1000Mb/s
48	ge-1/1/48	10/100/1000Mb/s
49	te-1/1/1	1Gb/s
50	te-1/1/2	1Gb/s
51	te-1/1/3	1Gb/s
52	te-1/1/4	1Gb/s

N8550-24CD8D Switch Port Name Description

NOTE:

For N8550-24CD8D, it supports thirty-two panel interfaces, which belong to four pipes, that is every eight panel ports (six 200G and two 400G ports) belong to one pipe. For only 18 ports are allowed to be split in one pipe, you need to split interfaces within this limitation. The corresponding relationship **of panel ports and pipes** is shown as below.

Table 1. Corresponding relationships of panel ports and pipes

pipe0	pipe1	pipe2	pipe3
1, 2, 3, 4, 5, 7, 26, 28	6, 8, 13, 15, 17, 19, 30, 32	9, 11, 18, 20, 21, 23, 27, 29	10, 12, 14, 16, 22, 24, 25, 31

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
2	xe-1/1/2	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
3	xe-1/1/3	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
4	xe-1/1/4	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
5	xe-1/1/5	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
6	xe-1/1/6	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
7	xe-1/1/7	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
8	xe-1/1/8	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
9	xe-1/1/9	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s

10	xe-1/1/10	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
11	xe-1/1/11	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
12	xe-1/1/12	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
13	xe-1/1/13	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
14	xe-1/1/14	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
15	xe-1/1/15	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
16	xe-1/1/16	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
17	xe-1/1/17	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
18	xe-1/1/18	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
19	xe-1/1/19	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
20	xe-1/1/20	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
21	xe-1/1/21	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
22	xe-1/1/22	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
23	xe-1/1/23	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s

24	xe-1/1/24	200Gb/s, 100Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
25	xe-1/1/25	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
26	xe-1/1/26	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
27	xe-1/1/27	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
28	xe-1/1/28	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
29	xe-1/1/29	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
30	xe-1/1/30	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
31	xe-1/1/31	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s
32	xe-1/1/32	400Gb/s, 200Gb/s, 100Gb/s, 4 x 100Gb/s, 2 x 200Gb/s, 4 x 50Gb/s, 2 x 100Gb/s, 4 x 25Gb/s, 2 x 50Gb/s

N9600-64OD Switch Port Name Description

NOTE:

After you split a port into 8 x 100Gb/s, another port in the same group can only be split into 2 x 400Gb/s or remains unsplit due to chip limitations.

A group is defined as two adjacent ports. For example:

- xe-1/1/1 and xe-1/1/2 form a group. If xe-1/1/1 is split into 8 x 100Gb/s, xe-1/1/2 can only be split into 2 x 400Gb/s or remains unsplit.
- Similarly, xe-1/1/3 and xe-1/1/4 form another group, xe-1/1/5 and xe-1/1/6 form another, and so on up to xe-1/1/59 and xe-1/1/60.

Mapping between physical ports, interface names and interface support speed are in the following table.

Physical Port Number	Interface Names	Interface Support Speed
1	xe-1/1/1	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
2	xe-1/1/2	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
3	xe-1/1/3	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
4	xe-1/1/4	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
5	xe-1/1/5	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
6	xe-1/1/6	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
7	xe-1/1/7	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
8	xe-1/1/8	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
9	xe-1/1/9	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

10	xe-1/1/10	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
11	xe-1/1/11	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
12	xe-1/1/12	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
13	xe-1/1/13	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
14	xe-1/1/14	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
15	xe-1/1/15	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
16	xe-1/1/16	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
17	xe-1/1/17	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
18	xe-1/1/18	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
19	xe-1/1/19	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
20	xe-1/1/20	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

21	xe-1/1/21	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
22	xe-1/1/22	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
23	xe-1/1/23	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
24	xe-1/1/24	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
25	xe-1/1/25	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
26	xe-1/1/26	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
27	xe-1/1/27	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
28	xe-1/1/28	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
29	xe-1/1/29	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
30	xe-1/1/30	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
31	xe-1/1/31	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

32	xe-1/1/32	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
33	xe-1/1/33	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
34	xe-1/1/34	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
35	xe-1/1/35	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
36	xe-1/1/36	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
37	xe-1/1/37	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
38	xe-1/1/38	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
39	xe-1/1/39	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
40	xe-1/1/40	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
41	xe-1/1/41	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
42	xe-1/1/42	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

43	xe-1/1/43	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
44	xe-1/1/44	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
45	xe-1/1/45	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
46	xe-1/1/46	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
47	xe-1/1/47	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
48	xe-1/1/48	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
49	xe-1/1/49	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
50	xe-1/1/50	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
51	xe-1/1/51	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
52	xe-1/1/52	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
53	xe-1/1/53	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

54	xe-1/1/54	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
55	xe-1/1/55	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
56	xe-1/1/56	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
57	xe-1/1/57	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
58	xe-1/1/58	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
59	xe-1/1/59	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s.

		Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
60	xe-1/1/60	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
61	xe-1/1/61	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
62	xe-1/1/62	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
63	xe-1/1/63	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.
64	xe-1/1/64	800Gb/s, 400Gb/s, 200Gb/s, 100Gb/s. Split speed: 2 x 400Gb/s, 4 x 200Gb/s, 8 x 100Gb/s. Reduced speed: 2 x 400Gb/s supports 200Gb/s and 100Gb/s; 4 x 200Gb/s supports 100Gb/s; 8 x 100Gb/s supports 50Gb/s.

Switch Installation

- Check the Installation Environment
- Install and Remove RPSU
- Install and Remove FRU
- Before Installation
- Installation
  - Install hangers, slide rail, grounding cable to the switch
  - Install the switch to the equipment cabinet
  - The Switch installation flow chart

Before Installation

Unpacking the Switch
Step 1 Carefully cut the tape that seals the shipping container, and open the top.
Step 2 Locate and remove the AC power cord kit.
Step 3 Lift the Switch from the container, and remove the two foam braces.
Step 4 Remove the antistatic bag from the Switch, and place the Switch on an antistatic mat.

Security Precaution
To ensure safe use and to prevent equipment damage, please follow the list below:

- Before cleaning switch, unplug the power cord.
- Prevent water or moisture from getting into the switch.
- Keep the vents unblocked.
- Ensure correct voltage is available.
- To reduce the risk of electric shock and to prevent electrostatic damage to components of the switch, do not open the cover when the switch is in use.

Check the Installation Environment

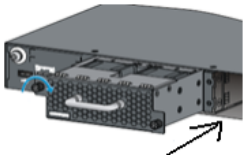
For proper and safe operation, the following conditions must be met prior to installation:

- Confirm that the cabinet itself has a good ventilation and cooling system.
- Confirm that the cabinet is strong enough to support the switches.
- Confirm that the cabinet is well grounded.
- To guarantee normal operation and service life of the switch, a stable temperature and humidity in the equipment room must be maintained.
- Keep the switch clean and maintain normal anti-interference standards.

Install and Remove FRU

The following instructions are used to replace an FRU (field-replaceable unit) on the switch:

1. Remove the faulty FRU from the switch.
2. Unpack the spare FRU, and double check to ensure that the FRU model is compatible with the switch.
3. Plug the FRU into the switch, moving slowly and using standard techniques to reduce electrostatic build-up.
4. Tighten the screws, and double check to make sure that the FRU is properly seated.

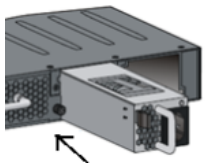


2-5-1 Installation FRU on switch schematic diagram
Remove FRU on the switch in the same way as installation.

Install and Remove RPSU

Installation of RPSU on the switch:
Step 1: Remove RPSU from the packaging box after ensuring the model is consistent with the switch.
Step 2: Plug the RPSU into the switch. Make sure the power supply module is in the right direction (from top to bottom).

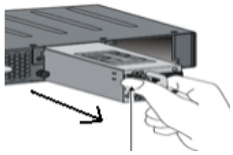
> In the process of plugging in the RPSU, move slowly and prevent electrostatic buildup using standard techniques.



2-4-1 Installation of RPSU on the switch schematic diagram.

Remove the RPSU from the switch in the same way. Remove the power line on the RPSU.

> In order to protect the RPSU, remove the RPSU on the anti-static bag.



2-4-2 Installation of RPSU on switch schematic diagram

> The P-3290 has only one RPSU. Its RPSU is fixed in the switch, so its RPSU cannot be plugged in and out.

Installation

- Install hangers, slide rail, grounding cable to the switch
- Install the switch to the equipment cabinet
- The Switch installation flow chart

Install hangers, slide rail, grounding cable to the switch

During the installation process, create adjustments according to requirements of installation, and select an appropriate location for hanging ears and grounding cable installations.

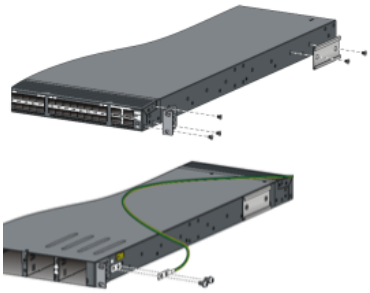
The instructions for how to install hanging ears and slide rails is as follows:

Step 1 Install the hangers to the case:
Line up the mounting holes of the hanging ears and the chassis side screw holes. Tighten the screws so that the hanging ears are fixed to the chassis.

Step 2 Install the slide guide rail to the chassis:

Line up the mounting holes of the slide guide rail and the side screw holes. Tighten the screws so that the slide guide rail is fixed to the chassis.

Step 3 Install the grounding screw, which connects the grounding cable to the screw holes.



2-1 Installation of hangers, slide rail and grounding cable diagram

Install the switch to the equipment cabinet

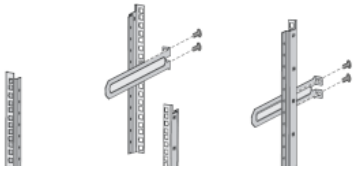
The instructions of how to install the switch on the cabinet is as follows:

Step 1 Allocate an area on the cabinet wherein the switch will be installed.

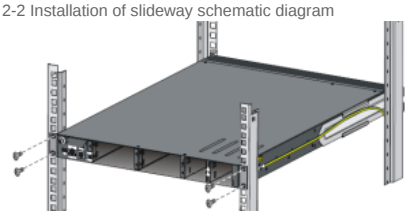
Step 2 Install the slideway on the equipment cabinet.

Step 3 Install the switch to the equipment cabinet. (Try to prevent electrostatic.)

> **NOTE:**
>
> For AG6248C, insert the external USB disk before installing the system, and install PicOS on the USB disk.

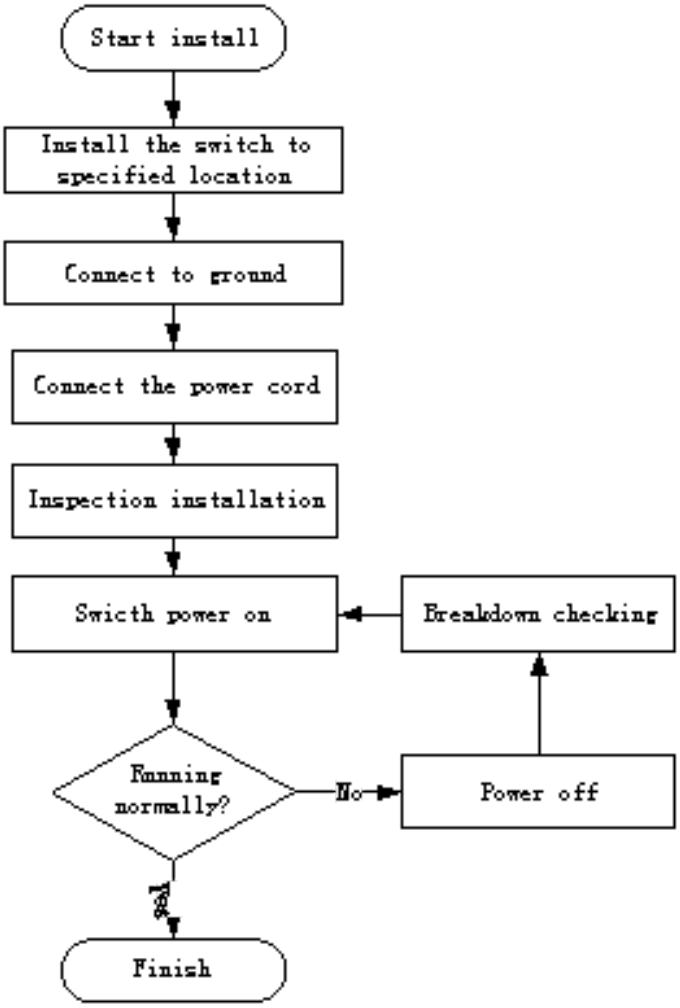


2-2 Installation of slideway schematic diagram



2-3 Installation the switch to the cabinet

The Switch installation flow chart



Flow Scalability per Broadcom Chipset

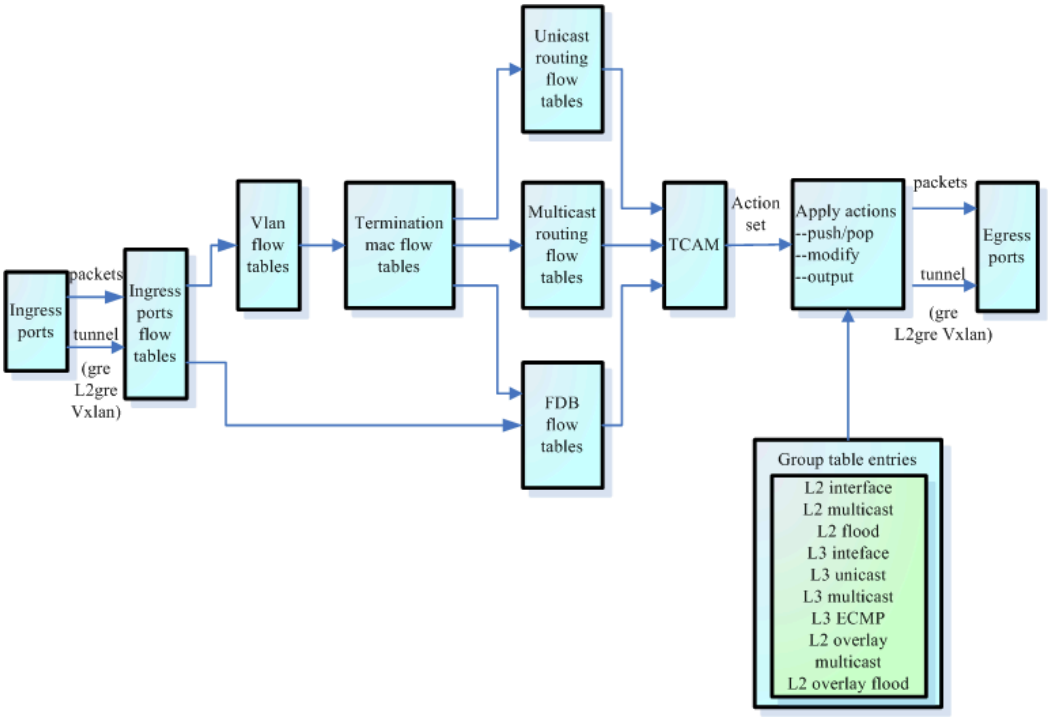
The maximum entries of OpenFlow Flows is often a critical piece of any SDN solution. This is a summary of Openflow Flow scalability per family of Chipset.

Chipset	ICAP (maximum entries in default or match modes)					ECAP (entries)	VCAP (entries)	L2 (maximum entries when buffer-mode is 5)	L3 (maximum entries when buffer-mode 5)			
	default	IPv4	IPv6	MAC	ARP				IPv4 host route	IPv4 forwarding route	IPv6 host route	IPv6 forwarding route
Helix4	2048	4096	2048	4096	2048	512	1024	32768	16384	6000	8192	3000
Trident 2	2048	4096	2048	4096	4096	512	512	32768	12000	12000	6000	6000
Trident 2+	8192	16384	8192	16384	16384	512	512	32768	12000	12000	6000	6000
Trident 3-X3	3072	3072	3072	3072	3072	512	1024	16384	12000	4000	6000	2000
Trident 3-X5	3072	3072	3072	3072	3072	1024	512	32768	12000	12000	6000	6000
Trident 3-X7	3072	3072	3072	3072	3072	1024	512	32768	12000	12000	6000	6000
Tomahawk/Tomahawk+	1024	3072	1024	3072	3072	512	512	8192	6500	12000	3250	6000
Tomahawk2	1024	3072	1024	3072	3072	512	512	8192	6500	12000	3250	6000
Maverick	4096	8192	4096	8192	8192	512	512	32768	4000	12000	2000	6000
Tomahawk3	1024	3072	1024	3072	3072	256	256	8192	16384	3840	8192	1920
Trident 4-X9	4096	4096	4096	4096	4096	1024	512	163840	12000	3072	6000	1536
Tomahawk5	1024	1024	1024	1024	1024	256	1024	8192	16384	491520	8192	245760

Switch Hardware Architecture

Most Top of Rack switches have the same general architecture. Once packets enter into a switch, they go through an ASIC "Pipeline" designed to make decisions on packets.

As an example, here is the simplified pipeline of a Broadcom chipset.



Here are definitions of the most common terminology to describe those architectures:

FIB - Forwarding Information Base or RoutingTable

FIB is a table memory used mainly to make IP destination prefix-based switching decisions.

The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

TCAM - Ternary Content-addressable Memory

Ternary content-addressable memory (TCAM) is a memory type used mainly for QOS or ACL.
A TCAM is a specialized type of high-speed memory that searches all of its contents in a single clock cycle. The term “ternary” refers to its ability to store and query data using three different inputs: 0, 1 and X.

In addition, most modern ASIC switch architecture supports the ability to perform multiple lookups into multiple distinct TCAM regions (or slices) in parallel. As a result of this ability to perform multiple lookups simultaneously, modern switches do not suffer any performance degradation by enabling additional hardware-switching features, such as QoS and IP ACL processing.

PICOS System Configuration Guide

- Getting Started
  - Boot Process and U-Boot Environment
  - Configuring Password for Entering Linux Shell
  - Initial Switch Access
  - The Default Login
- Quick Configuration Guide
  - Initial Setup
  - Basic Configuration
  - Network Configuration
    - Configuring an Interface
    - Configuring the Routing
  - Security Configuration
    - Configuring an ACL
    - Configuring the SSH Access
  - Typical Configuration Example
- Installing or Upgrading PICOS
  - ONIE Version and BIOS/U-Boot Information of Verified Platforms
  - Installing PICOS on Bare Metal Switches
  - Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command
  - Upgrading PICOS from Version 3.0 or Later Using Upgrade2
  - Installing Debian Packages on PICOS
    - Installing GCC on PicOS
    - Installing Puppet on PicOS
    - Installing Salt on PicOS
  - PICOS Installation and Upgrade Guide for FS S5810 Series, S3410 Series, S5860 Series and N8560-32C Switches
    - Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Console Port)
    - Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Console Port)
    - Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches
    - Installing PICOS for FS S3410 Series Switches
    - Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Eth0 or Inband Management Interface)
    - Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Eth0 or Inband Management Interface)
  - PICOS Debian Package Upgrade User Guide
- Zero Touch Provisioning (ZTP)
  - Overview of ZTP
    - ZTP Fundamentals
    - DHCP Configuration of ZTP
    - Provision Script
  - Enabling or Disabling ZTP
  - Preparation before ZTP Deployment
  - Example for Implementing ZTP Deployment through DHCP
  - Appendix: ZTP API
- PICOS Licenses
  - License Portal Guide
  - Installing License under Linux prompt
  - Installing and Removing License for PICOS go2cli Version
- PICOS Mode Selection
  - Changing PicOS Mode by Modifying the Boot File
  - PicOS Boot File
  - Changing PicOS Mode from CLI
- PICOS Password Recovery
  - Password Recovery for X86 Platform
  - Password Recovery for AS4610 Series Switches
  - Password Recovery Guide for FS S5810/S5860 Series Switches
  - Password Recovery Guide for FS N8560-32C
- Setting Date and Time
- Boot Diagnosis Report
- Rebooting the System
- Auto-Run Script Upon System Boot Up
- Sample for Crossflow OVS Remarking Rules with Auto-run Script
- Graceful Bootup with Backup Configuration
- IP Rule of Management Network and Service Network
- Display System EEPROM Data Block
- Manual File Backup
- PICOS Monitor
- Enable Web-based Management Interface
- Linux command: ssh/scp/ping/traceroute/apt-get/telnet

Getting Started

- Boot Process and U-Boot Environment
- Configuring Password for Entering Linux Shell
- Initial Switch Access
- The Default Login

Boot Process and U-Boot Environment

Before following the instructions in this section, user must have access to the switch console. User's terminal emulation software has to be configured with the following settings to ensure a successful console connection to the switch:

- **Baud rate:** 115200
- **Data bits:** 8
- **Stop bits:** 1

Modifying U-Boot Parameters

U-Boot (Universal Boot Loader) is an open source, primary boot loader for embedded devices. U-boot is used to package the instructions to boot the operating system kernel of a device. The following example shows the auto boot-up sequence:

```
U-Boot 1.3.0 (Sep 8 2014 - 16:39:03)
CPU:   8541, Version: 1.1, (0x80720011)
Core:  E500, Version: 2.4, (0x80200020)
Clock Configuration:
       CPU: 825 MHz, CCB: 330 MHz,
       DDR: 165 MHz, LBC:  41 MHz
L1:    D-cache 32 kB enabled
       I-cache 32 kB enabled
I2C:   ready
DRAM:  Initializing
initdram robin1
initdram robin2
robin before CFG_READ_SPD
robin after CFG_READ_SPD
initdram robin3
    DDR: 512 MB
FLASH: 32 MB
L2 cache 256KB: enabled
In:    serial
Out:   serial
Err:   serial
Net:   TSEC0, TSEC1
IDE:   Bus 0: OK
  Device 0: Model: CF 512MB Firm: 20060911 Ser#: TSS250160703090517 50
            Type: Hard Disk
            Capacity: 495.1 MB = 0.4 GB (1014048 x 512)
Hit any key to stop autoboot:  5
```

To modify the baud rate or other boot parameters, interrupt the boot sequence by hitting any key during auto boot. Once the boot sequence is interrupted, user is at the U-boot shell.

> Do not interrupt the default auto boot sequence unless the file system is being fixed or the console port settings are being changed.

The most common commands in U-Boot are:

- **help -** Get command line help.
- **printenv -** Show all environment variables. The U-Boot environment is a block of memory kept on persistent storage and copied to RAM when U-Boot starts. It stores environment variables used to configure the system.
- **version -** Show the U-Boot version.
- **setenv -** Set an environment variable.
- **saveenv -** Save the modification in the environment memory.

Use the **set** and **save** commands to reset the U-Boot environment variables. In the example below, the baud rate is set to 11520 with the **setenv baudrate 115200** command.

```
=> set baudrate 115200
=> save
Saving Environment to Flash...
Un-Protected 1 sectors
Erasing Flash...
. done
Erased 1 sectors
Writing to Flash... done
Protected 1 sectors
=> reset
```

PicOS switches do support Linux shutdown command. To shut down a switch, after running the “sudo shutdown -h now” command, disconnect the power supply.

Configuring Password for Entering Linux Shell

In CLI configure mode, you can use the following command to enter the Linux shell:

```
admin@PICOS# run start shell sh
admin@PICOS:~$
```

To enhance system security, PICOS supports setting a password for entering the Linux shell. The command **set system start-shell-sh password** can be used to configure the password when using command ***run start shell sh*** to entering Linux shell.

The configuration takes effect immediately after successfully commit.

When showing the configuration, the password is displayed as ciphertext.

Example

- Configure the password for entering Linux shell and enter Linux shell with this password.

```
admin@PICOS# set system start-shell-sh password 123456abc
admin@PICOS# commit
Commit OK.
Save done.
admin@PICOS# run start shell sh 123456abc
admin@PICOS:~$
```

Initial Switch Access

- Console Port
- Ethernet Management Port
- Assigning an IP Address to Management Interface
  - Configuring Management Interface
  - Configuration Example

Initial configuration of the switch requires user to connect either a terminal or a computer to the switch console port. Once user gets access to the switch and establishes CLI (command-line interface) over the serial console connection, then assign an IP address to the management port and create an IP route to the gateway. Keep the following points in mind:

- The console port provides local serial access to the switch.
- The Ethernet management port is used for out-of-band network management tasks. Before using the management port for the first time, an IP address must be assigned to that port.

Console Port

The console port is located at the front of the switch, as shown in Figure 1. User can connect a terminal or a computer to the console port using a serial or RS-232 cable. The accessory kit includes an RJ45 to DB9 adapter cable.

Port Settings

Use the following port settings to connect a terminal or a computer to the switch console port:

Baud rate: 115200

Data bits: 8

Stop bits: 1

The default width for a terminal session through the console port is 80 characters. That means that the width of the terminal client should be a minimum of 80 characters to properly use the console port. Most terminal client default width is 80 characters.

Ethernet Management Port

Pica8 switches provide one or two Ethernet management ports for switch configuration and out-of-band network management. Please see Figure 1, which shows the console and management ports of the Pica8 P-3930 switch. The port labelled *ETHERNET* is the management port, while the port labelled *CONSOLE* is the console port.

Figure 1 Console and Management Ports



Assigning an IP Address to Management Interface

Once granted initial access to the switch, user needs to configure the management IP address and default gateway in either L2/L3 mode or OVS mode. This section describes the configurarion in L2/L3 mode.

For detail of configuration in OVS mode, please refer to Configuring IP addressing in OVS mode.

The management IP address is used to maintain and manage the device. You can configure the management interface eth0 with static IP addresses or through dynamic address allocation using DHCP. If the static IP address is not assigned, the system will try to obtain the management port IP address dynamically from the DHCP server by default.

> **NOTE:**
>
> When switching from OVS mode to L2/L3 mode, the static IP address of the management port configured before will still be used if there is no user configuration for it in the new mode.

Configuring Management Interface

Step1 Set static IP addresses for management interface eth0.

set system management-ethernet eth0 ip-address {**IPv4** | **IPv6}** <*ip_address*>

> **NOTE:**
>
> If the static IP address is not assigned, the system will try to dynamically obtain the management port IP address from the DHCP server which is also the factory setting.

Step2 Set the gateway address for management interface eth0.

set system management-ethernet eth0 ip-gateway {**IPv4** | **IPv6}** <*ip_address*>

Configuration Example

Step1 Set static IP addresses for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-address IPv4 192.168.10.5/24
```

Step2 Set the gateway address for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-gateway IPv4 192.168.10.1
```

Step3 Commit the configuration.

```
admin@XorPlus# commit
```

Step4 Verify the configuration.

- Run **run show system management-ethernet** command to view the configuration information, status and traffic statistics information of the management interface.

```
admin@XorPlus# run show system management-ethernet
eth0     Hwaddr: 00:18:23:30:e5:72       State: UP
               Gateway  : 192.168.10.1
               Inet addr:
                   192.168.10.5/24
       Traffic statistics
               Input Packets.....................3620
               Input Bytes.......................462971
               Output Packets....................597
               Output Bytes......................75459
```

The Default Login

The Pica8 PicOS software operates in two modes.

L2/L3 (Layer 2/Layer 3) Mode: This is the default PicOS mode. In this mode, the switch is used for traditional Layer 2 switching and Layer 3 routing. The OVS daemon is ***not*** running in the L2/L3 mode.

OVS (Open vSwitch) Mode: In this mode, the switch is completely dedicated to Open vSwitch and the L2/L3 daemon is ***not*** running.

By default PicOS has two users, **root** and **admin**.

Password for the **admin** account must be manually set during the first login. User should use **pica8** as the password at first login. Then, the system will prompt user to change the default password. The new password is a string of 8 to 512 case-sensitive characters.



The PICOS Password Recovery process is available in the event of a forgotten password.

```
PICOS login: admin
Password: (input default password "pica8")
You are required to change your password immediately (administrator enforced)
Changing password for admin.
Current password: (input "pica8" again)
New password: (input new password: the new password should be no less than eight characters)
Retype new password: (input new password again)
Linux PICOS 5.10.23 #2 SMP Mon Aug 12 09:14:57 CST 2024 x86_64
Synchronizing configuration...OK.
Welcome to PICOS
admin@PICOS>
```

PICOS go2cli Version

For PICOS **go2cli** version, users login to the operation mode of PICOS CLI:

```
admin@PICOS>
```

At PICOS CLI prompt, run **start shell sh** to enter Linux shell.

```
admin@PICOS> start shell sh
admin@PICOS:~$
```

After entering Linux shell, user should use **sudo su** switch to **root** without a password.

```
admin@PICOS>
admin@PICOS> start shell sh
admin@PICOS:~$ sudo su
root@PICOS:/home/admin#
```

If you want to return from the Linux shell back to the CLI prompt, run "**exit**".

```
admin@PICOS:~$ exit
exit

admin@PICOS>
```

SSH Access to the Switch

After the switch starts up, the management interface (*eth0* or *inband-mgmt*) will be assigned an IP address by DHCP server or use factory default IP *192.168.1.1/24*. You can log in to the switch with this IP through SSH, the operation details are shown below.

Step 1 Users can check the management IP address through `ifconfig`.

```
admin@PICOS:~$ ifconfig
bridge0   Link encap:Ethernet  HWaddr 64:9D:99:D8:FD:09
          inet6 addr: fe80::669d:99ff:fed8:fd09/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:65535  Metric:1
          RX packets:279516 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:98589775 (94.0 MiB)  TX bytes:7599297 (7.2 MiB)

ge1       Link encap:Ethernet  HWaddr 64:9D:99:D8:FD:07
          inet6 addr: fe80::669d:99ff:fed8:fd07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:65521  Metric:1
          RX packets:279516 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:103621063 (98.8 MiB)  TX bytes:8248541 (7.8 MiB)

inband-mgmt Link encap:Ethernet  HWaddr 64:9D:99:D8:FD:07
          inet addr:10.10.51.159  Bcast:10.10.51.255  Mask:255.255.255.0
          inet6 addr: fe80::669d:99ff:fed8:fd07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:279433 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:98578866 (94.0 MiB)  TX bytes:7598551 (7.2 MiB)
```

Step 2 You can log in to the switch with this IP through SSH.

```
C:\Users\Administrator>ssh admin@10.10.51.159
```

Connection Management

Pica8 switches support three connection methods:

- Console
- SSH

> By default, console and SSH are *enabled*.

Log in via console port:

The following example shows how user can connect to a switch via SSH with *admin* as username:

```
admin@PICOS> ssh 192.168.50.10 -l admin
admin@192.168.50.10's password:
Last login: Mon Oct 14 08:23:27 2024
Synchronizing configuration...OK.
Welcome to PICOS
admin@PICOS>
```

> By default, root login is disabled via SSH.

The following example enables *root* login via SSH:

```
admin@PICOS# set system services ssh root-login  allow
admin@PICOS# commit
Commit OK.
Save done.
```

⚠ The root user account password is locked (non-existent). If logging in via root, user needs to reset the password.

By default, a SSH session is never terminated. However, user can set a time limit for idle sessions. In other words, if a session is idle for certain time, it will automatically be terminated. Use the **set cli idle-timeout** command, in L2/L3 mode, to configure the maximum time in minutes a session can stay idle before it is terminated.

```
PICOS login: admin
Password:
Linux PICOS 5.10.23 #2 SMP Mon Aug 12 09:14:57 CST 2024 x86_64
Last login: Mon Oct 14 07:25:53 UTC 2024 on ttyS0
Synchronizing configuration...OK.
Welcome to PICOS
admin@PICOS> set cli idle-timeout 10
admin@PICOS>
```

Quick Configuration Guide

- Initial Setup
- Basic Configuration
- Network Configuration
- Security Configuration
- Typical Configuration Example

Initial Setup

Before performing the following operations, you should make sure that the device has been installed successfully. For detailed information of installing PicOS, see Installing or Upgrading PICOS.

Powering on the Switch

Logging in Switch through the Console Port

Powering on the Switch

Connect the switch to a power supply through the power cord, and then press the power button to power on the switch.

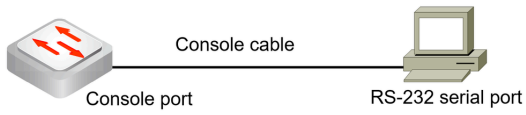
Logging in Switch through the Console Port

For initial system configuration, you should connect the switch to a terminal through the Console port.

Procedure

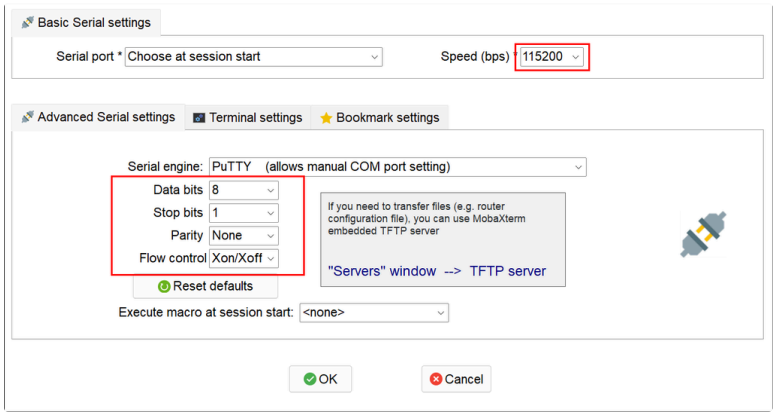
Step1 Connect the console port of the switch to the serial port of a PC through a console cable, as shown in the figure below.

Figure 1. Connetion of Console cable



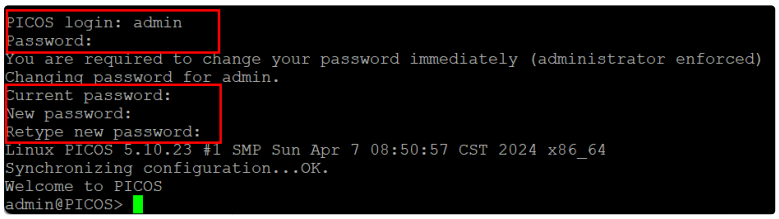
Step2 Open a terminal emulator (e.g., PuTTY) and configure it with the appropriate COM port settings, which should be the same with the switch related parameters. As shown in the figure below.

Figure 2. Serial Settings of Terminal Emulator



Step3 Enter the default administrator name **admin** and password **pica8** at the **PICOS login** and **password** prompts, and press **Enter**. Change the default password according to prompts, press **Enter**, and you can successfully log in CLI. As shown in the figure below.

Figure 3. Password Modification for First login


PICOS login: admin
Password:
You are required to change your password immediately (administrator enforced)
Changing password for admin.
Current password:
New password:
Retype new password:
Linux PICOS 5.10.23 #1 SMP Sun Apr 7 08:50:57 CST 2024 x86_64
Synchronizing configuration...OK.
Welcome to PICOS
admin@PICOS>

Basic Configuration

- Entering CLI Configuration Mode
- Configuring a Host Name
- Configuring the Management IP Address

Entering CLI Configuration Mode

PicOS supports different CLI modes, which are indicated by different prompts. Some commands can only be run in certain modes.

- Operation mode

When log in PicOS CLI, you are in the operation mode by default. You can execute some basic configurations in this mode, such as clear and show, etc. **>** indicates the operation mode, as shown in the figure below.

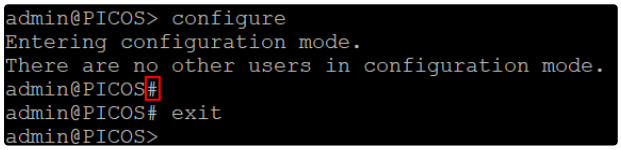
Figure 1. Prompt of Operation Mode



- Configuration mode

You can configure the switch function in this mode, such as interface, routing, etc. Run **configure** in the operation mode to enter the configuration mode, and run **exit** to return to the operation mode. **#** indicates the configuration mode, as shown in the figure below.

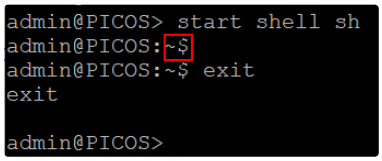
Figure 2. Prompt of Configuration Mode



- Linux shell mode

Run **start shell sh** in the operation mode to enter the Linux shell mode, and run **exit** to return to the operation mode. **~$** indicates the Linux shell mode, as shown in the figure below.

Figure 3. Prompt of Linux Shell Mode



After restarting PICOS using the command `sudo systemctl restart picos` in the Linux shell, entering `exit` will disconnect the current SSH session, requiring the user to log in again to access the device.

Configuring a Host Name

Overview

A host name distinguishes one device from another. The default host name is the system name PICOS. You can modify the host name as required.

Procedure

Step1 In the configuration mode, specify or modify a host name for the switch.

```
set system hostname <hostname>
```

Step2 Commit the configuration.

```
commit
```

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show system name** command to view the new host name.

Other Configurations

To reset the hostname to default, use **delete system hostname** command.

Configuring the Management IP Address

Overview

To facilitate the device management and meet the requirement of separating the management traffic from the data traffic, the switch supports the in-band or out-of-band management interface with the factory default IP address 192.168.1.1/24. If the switch cannot obtain the IP address through DHCP, the factory default IP address is valid, and you can access it through PCs in the same network segment. Besides, you can manually configure the IP address as needed.

Procedure

Step1 In the configuration mode, specify the IP address for management interface.

```
set system management-ethernet eth0 ip-address {IPv4 | IPv6} <ip-address>

set l3-interface vlan-interface inband-mgmt address <ipv4-address | ipv6-address> prefix-length
<length>
```

Step2 Commit the configuration.

```
commit
```

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show system management-ethernet** command to view the MAC address, IP address, state and traffic statistics.

Other Configurations

To clear the configuration of management interface, use **delete system management-ethernet eth0 ip-address** command.

Network Configuration

- Configuring an Interface
- Configuring the Routing

Configuring an Interface

Interfaces are used to exchange data and communicate with other network devices, which include physical interfaces and logical interfaces.

- Physical interface: exists on interface cards, which can be used for management and service.
  - Management interface: the switch supports a management interface eth0 by default, which is used to log in devices for configuration and management. For detailed information for the management interface, see Configuring the Management IP Address.
  - Service interface: can be used for service transmission, which includes Layer 2 Ethernet interfaces and Layer 3 Ethernet interfaces. By default, service interfaces of switch are all Layer 2 interfaces. To configure a Layer 2 interface as a Layer 3 interface, see the following chapter.
- Logical interface: not exists physically and is configured manually, which is used for service transmission. It includes Layer 3 interfaces, routed interfaces, loopback interfaces, etc.

It includes the following chapters:

- Configuring a loopback interface
- Configuring a Routed interface
- Configuring a VLAN Interface

Configuring a loopback interface

Overview

The loopback interface is always up to ensure network reliability, which has the following features:

- It is always up and has the loopback feature.
- It can be configured with the mask of all 1s.

Based on the features, the loopback interface has the following applications:

- The IP address of a loopback interface is specified as the source address of packets to improve network reliability.
- When no Router ID is configured for dynamic routing protocols, the maximum IP address of the loopback interface is configured as the router ID automatically.

Procedure

Step1 In the configuration mode, specify the name and IP address for the loopback interface.

```
set l3-interface loopback <loopback-name> address <ipv4-address> prefix-length 32
set l3-interface loopback <loopback-name> address <ipv6-address> prefix-length 128
```

Step2 Commit the configuration.

```
commit
```

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface loopback** <*loopback-name*> command to view the state, IP address, description and traffic statistics.

Other Configurations

By default, the loopback interface is enabled when created. To disable the loopback interface, use **set l3-interface loopback** <*interface-name*> **disable** command.

To clear the configuration of loopback interface, use **delete l3-interface loopback interface** <*interface-name*> command.

Configuring a Routed interface

Overview

All Ethernet ports of switch are Layer 2 interfaces by default. When you need to use an Ethernet port for Layer 3 communication, you can enable the Ethernet port as a routed interface. The routed interface is a Layer 3 interface which can be assigned an IP address and can be configured with a routing protocol to connect to other Layer 3 routing devices.

Procedure

Step1 In the configuration mode, set reserved VLANs for the use of routed interface.

set vlans reserved-vlan <*reserved-vlan*>

- **reserved-vlan** <*reserved-vlan*>: specifies the reserved VLANs. The valid VLAN numbers range is 2-4094. User can specify a range of VLAN numbers, e.g. 2,3,50-100. System supports up to 128 reserved VLANs.

Step2 Select a physical interface as the routed interface and specify a name.

set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

- **routed-interface name** <*string*>**:** specifies a routed interface name.

The name must start with "rif-", for example, rif-ge1.

Step3 Enable the routed interface.

set interface gigabit-ethernet <*interface-name*> **routed-interface enable true**

Step4 Configure an IP address for the routed interface.

set l3-interface routed-interface <*string*> **address** <*ipv4-address* | *ipv6-address*> **prefix-length** <*prefix-number*>

- **prefix-length** <*prefix-number*>: specifies the network prefix length. The range is 4-32 for IPv4 address, and 1-128 for IPv6 address.

Step5 Commit the configuration.

commit

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface routed-interface** <*interface-name*> command to view the state, IP address, MAC address, VLAN, MTU, description and traffic statistics.

Other Configurations

To disable the routed interface, use **set interface gigabit-ethernet** <*interface-name*> command.

Configuring a VLAN Interface

Overview

By default, the native VLAN of all physical interfaces is VLAN 1, which can implement Layer 2 communication. To implement Layer 3 communication between users in different VLANs and network segments, you can configure the VLAN interface, which is a Layer 3 logical interface.

Procedure

Step1 In the configuration mode, create a VLAN.

The VLAN ID has been pre-configured in system from version 4.3.2 and you don't need to configure it.

set vlans vlan-id <*vlan-id*>

- **vlan-id** <*vlan-id*>: specifies the VLAN tag identifier. The valid VLAN numbers range 1-4094. User can specify a range of VLAN numbers, e.g. 2,3,5-100.

Step2 Specify the created VLAN as the native VLAN for a physical interface.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching native-vlan-id** <*vlan-id*>

Step3 Associate a Layer 3 interface with the VLAN.

set vlans vlan-id <*vlan-id*> **l3-interface** <*interface-name*>

- **l3-interface** <*interface-name*>*:* specifies a name for the Layer 3 interface.

Step4 Configure an IP address for the VLAN interface.

set l3-interface vlan-interface <*interface-name*> **address** <*ipv4-address* | *ipv6-address*> **prefix-length** <*prefix-number*>

Step5 Commit the configuration.

commit

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface vlan-interface** <*interface-name*> command to view the state, IP address, MAC address, VLAN, MTU, description and traffic statistics.

Other Configurations

To clear the configuration of VLAN interface, use **delete l3-interface vlan-interface** <*interface-name*> command.

Configuring the Routing

Routing is a process of forwarding packets from one network to a destination address in another network. The implement of route selection and packet forwarding is based on various routes stored in the routing table. To maintain the routing table, you can manually add or configure different routing protocols.

The switch supports direct routing, static routing and dynamic routing.

- Direct routing: discovered by a data link layer protocol.
- Static routing: manually configured.
- Dynamic routing: discovered by a dynamic routing protocol.

It includes the following chapters:

- Configuring the Static Routing
- Configuring the Dynamic Routing

Configuring the Static Routing

Overview

The static routing is manually configured, which requires low system performance and is applicable to small-size network with simple and stable topologies.

Procedure

Before configuring the routing, make sure that the Layer 3 interface has been configured.

Step1 By default, the IP routing function is disabled. In the configuration mode, enable the IP routing function.

```
set ip routing enable true
```

Step2 Specify the destination address, and configure one of next-hop IP address and outgoing interface as needed.

set protocols static route <*ip/prefixlen*> **next-hop** <*nexthop-address*>

- **route** <*ip/prefixlen*>: specifies a destination IPv4 or IPv6 address and the prefix length of 1 to 32 for IPv4 and 1 to 128 for IPv6.
- **next-hop** <*nexthop-address*>: specifies the next-hop IP address.

set protocols static interface-route <*ip/prefixlen*> **interface** <*interface-name*>

- **interface** <*interface-name*>: specifies the Layer 3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.

Step3 Commit the configuration.

```
commit
```

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show route static** command to view all static routing entries.

Other Configurations

To clear the configuration of static interface, use **delete protocols static route**<*ip/prefixlen*> command.

Configuring the Dynamic Routing

The dynamic routing is based on algorithm, which requires higher system performance. It is applicable to network with a large number of Layer 3 devices, and can automatically adapt to the changeable network topology.

The switch supports multiple dynamic routing, such as OSPF, BGP, IS-IS, etc. OSPF is the IGP (Interior Gateway Protocol) recommended by PicOS. Take the OSPF routing as an example to introduce how to configure a dynamic routing.

Overview

OSPF (Open Shortest Path First) is developed by IETF (Internet Engineering Task Force), which uses the shortest path first (SPF) algorithm to calculate a shortest path tree (SPT) to all destination addresses based on the network topology, and is advertised through link state advertisements (LSAs). It is applicable to the network with several hundred devices, such as small and medium-sized enterprises networks.

PicOS supports OSPFv2 and OSPFv3, which is respectively intended for IPv4 and IPv6.

Procedure

Before configuring the routing, make sure that the Layer 3 interface has been configured.

Step1 By default, the IP routing function is disabled. In the configuration mode, enable the IP routing function.

set ip routing enable true

Step2 Set the OSPF router ID.

set protocols ospf router-id <*router-id*>

- **router-id** <*router-id*>: specifies the OSPF router ID, which can uniquely identify the switch within the domain. The value is in IPv4 dotted decimal format.

Step3 Add the specified network segment to an area. Area 0 is required.

set protocols ospf network <*ipv4/prefixlen*> **area** {<*area-id* | *ipv4*>}

- **network** <*ipv4/prefixlen*>: specifies the network prefix and prefix length in IPv4 format.
- **area** {<*area-id* | *ipv4*>}: specifies the OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Step4 Commit the configuration.

commit

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show route ospf** command to view all OSPF routing entries.

Other Configurations

To delete the OSPF routing configuration, use **delete protocols ospf** command.

Security Configuration

- Configuring an ACL
- Configuring the SSH Access

Configuring an ACL

Overview

ACL (Access Control List) is packet filtering rules through defining conditions of source addresses, destination addresses, interfaces, etc. The switch permits or denies packets according to the configured action of ACL rules.

ACL can manage network access behaviors, prevent network attacks, and improve bandwidth utilization through accurately identifying and controlling packets, which ensures network security and service quality.

Procedure

Step1 Set the sequence number of priority.

set firewall filter <*filter-name*> **sequence** <*sequence-number*>

- **sequence** <*sequence-number*>: specifies the sequence number. Smaller values represent higher priorities. The range is 0-9999.

Step2 Specify the source address and source port to filter matched packets.

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **from** {**source-address-ipv4** <*address/prefix-length*> | **source-address-ipv6** < *address/prefix-length* > | **source-mac-address** <*mac-address*> | **source-port** <*port-number*>}

- **source-port** <*port-number*>: specifies the source port number or port number range, for example, 5000 or 7000..7050.

Step3 Specify the execution action for packets matching the filter.

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **then action** {**discard** | **forward**}

- **action** {**discard** | **forward**}: discards or forwards matched packets.

Step4 Specify the physical interface, VLAN interface or routed interface to filter matched incoming and egress packets.

set firewall filter <*filter-name*> **input** {**interface** <*interface-name* > | **vlan-interface** <*vlan-interface-name*> | **routed-interface** <*routed-interface-name*>}

set firewall filter <*filter-name*> **output** {**interface** <*interface-name*> | **vlan-interface** <*vlan-interface-name*> | **routed-interface** <*routed-interface-name*>}

Step5 Commit the configuration.

commit

Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show filter** <*filter-name*> **[sequence** <*sequence-number*>] command to view the matching condition of specified filter.

Other Configurations

To delete the configured filter, use **delete firewall filter**<*filter-name*> command.

Configuring the SSH Access

Overview

SSH (Secure Shell) is an encryption network protocol, which can perform secure access and file transmission in the unsecured network. It performs data exchange through a secure channel, which is established based on TCP. The default port is 22, which can be changed as required for security purposes.

Procedure

By default, the SSH service is enabled. You can log in switch through SSH protocol by directly access eth0. Besides, if you want to remotely log in and manage the switch through the Layer 3 interface, you should configure as follows:

Step1 In the configuration mode, specify the loopback interface, VLAN interface or routed interface as the inband management port, both management traffic and data plane traffic can be transmitted through the specified interface. The specified interface should be in the default VRF.

set system inband {**loopback** <*ip-address*> | **vlan-interface** <*vlan-interface-name*> | **routed-interface** <*routed-interface-name*>}

Step2 (Optional) Set the limit number of SSH connections.

set system services ssh connection-limit <*int*>

- **connection-limit** <*int*>: specifies the maximum number of allowed connections, the valid number ranges 0-250. Default value is 0, which removes the connection limit.

Step3 (Optional) Specify the listening port number of SSH server.

set system services ssh port <*port-number*>

- **port** <*port-number*>: specifies the listening port number of the SSH server. The value is an integer ranging from 1 to 65535. Th default value is 22.

Step4 Commit the configuration.

commit

Verifying the Configuration

After the configuration is completed, use **ssh admin**@<*ip-address*> **-p** <*port*> to check whether the switch can be accessed through SSH.

Other Configurations

To disable the SSH service, use **set system services ssh disable true** command.

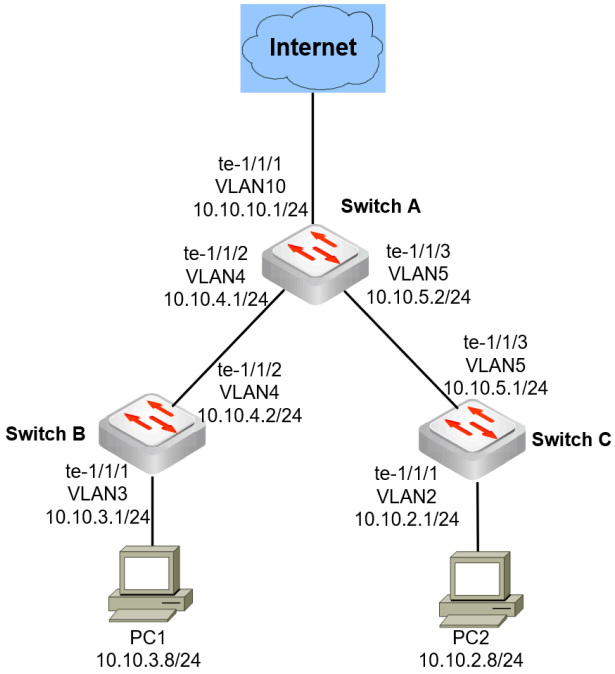
To delete the SSH configuration, use **delete system services ssh** command.

Typical Configuration Example

Overview

Take the following topology as an example to introduce how to implement communication between PC1 and PC2.

Figure 1. Topology of Access Network



The data plan is shown as below.

Device	Interface	VLAN and IP Address	
Switch A	te-1/1/1	VLAN: 10	IP address: 10.10.10.1/24
	te-1/1/2	VLAN: 4	IP address: 10.10.4.1/24
	te-1/1/3	VLAN: 5	IP address: 10.10.5.2/24
Switch B	te-1/1/1	VLAN: 3	IP address: 10.10.3.1/24
	te-1/1/2	VLAN: 4	IP address: 10.10.4.2/24
Switch C	te-1/1/1	VLAN: 2	IP address: 10.10.2.1/24
	te-1/1/3	VLAN: 5	IP address: 10.10.5.1/24
PC1	10.10.3.8/24		
PC2	10.10.2.8/24		

Procedure

Before configuring the following steps, make sure you have logged in the specified switch through Console port or SSH. For detailed information, see Initial Setup and Configuring the SSH Access.

Step1 In the configuration mode, configure the host name of switch respectively as SwitchA, SwitchB and SwitchC.

```
admin@PICOS> configure
admin@PICOS# set system hostname SwitchA
admin@PICOS# commit
admin@SwitchA#
```

Run the same command on other switches to change the hostname as SwitchB and SwitchC.

Step2 Configure the interface and VLAN.

- **Switch A**

Interface te-1-1-1:

```
admin@SwitchA# set vlans vlan-id 10
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchA# set l3-interface vlan-interface vlan10 address 10.10.10.1 prefix-length 24
admin@SwitchA# commit
```

Interface te-1-1-2:

```
admin@SwitchA# set vlans vlan-id 4
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 4
admin@SwitchA# set vlans vlan-id 4 l3-interface vlan4
admin@SwitchA# set l3-interface vlan-interface vlan4 address 10.10.4.1 prefix-length 24
admin@SwitchA# commit
```

Interface te-1-1-3:

```
admin@SwitchA# set vlans vlan-id 5
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 5
admin@SwitchA# set vlans vlan-id 5 l3-interface vlan5
admin@SwitchA# set l3-interface vlan-interface vlan5 address 10.10.5.2 prefix-length 24
admin@SwitchA# commit
```

- **Switch B**

Interface te-1-1-1:

```
admin@SwitchB# set vlans vlan-id 3
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 3
admin@SwitchB# set vlans vlan-id 3 l3-interface vlan3
admin@SwitchB# set l3-interface vlan-interface vlan3 address 10.10.3.1 prefix-length 24
admin@SwitchB# commit
```

Interface te-1-1-2:

```
admin@SwitchB# set vlans vlan-id 4
admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 4
admin@SwitchB# set vlans vlan-id 4 l3-interface vlan4
admin@SwitchB# set l3-interface vlan-interface vlan4 address 10.10.4.2 prefix-length 24
admin@SwitchB# commit
```

- **Switch C**

Interface te-1-1-1:

```
admin@SwitchC# set vlans vlan-id 2
admin@SwitchC# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2
admin@SwitchC# set vlans vlan-id 2 l3-interface vlan2
admin@SwitchC# set l3-interface vlan-interface vlan2 address 10.10.2.1 prefix-length 24
admin@SwitchC# commit
```

Interface te-1-1-3:

```
admin@SwitchC# set vlans vlan-id 5
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 5
admin@SwitchC# set vlans vlan-id 5 l3-interface vlan5
admin@SwitchC# set l3-interface vlan-interface vlan5 address 10.10.5.1 prefix-length 24
admin@SwitchC# commit
```

Step3 Configure the IP address and default gateway of PC1 and PC2.

PC1:

```
PC1> ip 10.10.3.8 255.255.255.0 10.10.3.1
Checking for duplicate address...
PC1 : 10.10.3.8 255.255.255.0 gateway 10.10.3.1
```

PC2:

```
PC2> ip 10.10.2.8 255.255.255.0 10.10.2.1
Checking for duplicate address...
PC2 : 10.10.2.8 255.255.255.0 gateway 10.10.2.1
```

Step4 Configure the routing. You can configure the static routing or OSPF routing to connect network.

- **Connecting network through the static routing**

Switch A:

```
admin@SwitchA# set ip routing enable true
admin@SwitchA# set protocols static route 10.10.2.0/24 next-hop 10.10.5.1
admin@SwitchA# set protocols static route 10.10.3.0/24 next-hop 10.10.4.2
admin@SwitchA# commit
```

Switch B:

```
admin@SwitchB# set ip routing enable true
admin@SwitchB# set protocols static route 0.0.0.0/0 next-hop 10.10.4.1
admin@SwitchB# commit
```

Switch C:

```
admin@SwitchC# set ip routing enable true
admin@SwitchC# set protocols static route 0.0.0.0/0 next-hop 10.10.5.2
admin@SwitchC# commit
```

- **Connecting network through the OSPF routing**

Switch A:

```
admin@SwitchA# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf network 10.10.4.0/24 area 0
admin@SwitchA# set protocols ospf network 10.10.10.0/24 area 0
```

```
admin@SwitchA# set protocols ospf network 10.10.5.0/24 area 1
admin@SwitchA# commit
```

Switch B:

```
admin@SwitchB# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@SwitchB# set protocols ospf router-id 2.2.2.2
admin@SwitchB# set protocols ospf network 10.10.4.0/24 area 0
admin@SwitchB# set protocols ospf network 10.10.3.0/24 area 0
admin@SwitchB# commit
```

Switch C:

```
admin@SwitchC# set l3-interface loopback lo address 3.3.3.3 prefix-length 32
admin@SwitchC# set protocols ospf router-id 3.3.3.3
admin@SwitchC# set protocols ospf network 10.10.2.0/24 area 1
admin@SwitchC# set protocols ospf network 10.10.5.0/24 area 1
admin@SwitchC# commit
```

Verifying the Configuration

- **View the routing table of each switch.**

1. Static Routing:

Figure2. Static Routing Entries of SwitchA

```
admin@SwitchA# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 10.10.2.0/24 [1/0] via 10.10.5.1, vlan5, weight 1, 00:07:36
S>* 10.10.3.0/24 [1/0] via 10.10.4.2, vlan4, weight 1, 00:07:36
```

Figure3. Static Routing Entries of SwitchB

```
admin@SwicthB# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 10.10.4.1, vlan4, weight 1, 00:10:38
```

Figure4. Static Routing Entries of SwitchC

```
admin@SwitchC# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 10.10.5.2, vlan5, weight 1, 00:13:07
```

2. OSPF Routing:

Figure5. OSPF Routing Entries of SwitchA

```
admin@SwitchA# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O>* 10.10.2.0/24 [110/200] via 10.10.5.1, vlan5, weight 1, 00:05:42
O>* 10.10.3.0/24 [110/200] via 10.10.4.2, vlan4, weight 1, 00:05:42
O   10.10.4.0/24 [110/100] is directly connected, vlan4, weight 1, 00:05:52
O   10.10.5.0/24 [110/100] is directly connected, vlan5, weight 1, 00:06:30
O   10.10.10.0/24 [110/100] is directly connected, vlan10, weight 1, 00:06:30
```

Figure6. OSPF Routing Entries of SwitchB

```
admin@SwitchB# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O>* 10.10.2.0/24 [110/300] via 10.10.4.1, vlan4, weight 1, 00:10:41
O   10.10.3.0/24 [110/100] is directly connected, vlan3, weight 1, 00:11:27
O   10.10.4.0/24 [110/100] is directly connected, vlan4, weight 1, 00:11:27
O>* 10.10.5.0/24 [110/200] via 10.10.4.1, vlan4, weight 1, 00:10:41
O>* 10.10.10.0/24 [110/200] via 10.10.4.1, vlan4, weight 1, 00:10:41
```

Figure7. OSPF Routing Entries of SwitchC

```
admin@SwitchC# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   10.10.2.0/24 [110/100] is directly connected, vlan2, weight 1, 00:14:17
O>* 10.10.3.0/24 [110/300] via 10.10.5.2, vlan5, weight 1, 00:13:32
O>* 10.10.4.0/24 [110/200] via 10.10.5.2, vlan5, weight 1, 00:13:32
O   10.10.5.0/24 [110/100] is directly connected, vlan5, weight 1, 00:14:16
O>* 10.10.10.0/24 [110/200] via 10.10.5.2, vlan5, weight 1, 00:13:32
```

- **Run Ping command to check the connectivity between PC1 and PC2.**

1. PC1 ping PC2:

Figure8. Result of PC1 Ping PC2

```
root@UbuntuDockerGuest-1:~# ping 10.10.2.8
PING 10.10.2.8 (10.10.2.8) 56(84) bytes of data.
64 bytes from 10.10.2.8: icmp_seq=1 ttl=61 time=29.1 ms
64 bytes from 10.10.2.8: icmp_seq=2 ttl=61 time=1.99 ms
64 bytes from 10.10.2.8: icmp_seq=3 ttl=61 time=2.29 ms
64 bytes from 10.10.2.8: icmp_seq=4 ttl=61 time=3.27 ms
64 bytes from 10.10.2.8: icmp_seq=5 ttl=61 time=3.92 ms
64 bytes from 10.10.2.8: icmp_seq=6 ttl=61 time=2.44 ms
```

2. PC2 ping PC1:

Figure9. Result of PC2 Ping PC1

```
root@UbuntuDockerGuest-2:~# ping 10.10.3.8
PING 10.10.3.8 (10.10.3.8) 56(84) bytes of data.
64 bytes from 10.10.3.8: icmp_seq=1 ttl=61 time=2.01 ms
64 bytes from 10.10.3.8: icmp_seq=2 ttl=61 time=2.92 ms
64 bytes from 10.10.3.8: icmp_seq=3 ttl=61 time=2.53 ms
64 bytes from 10.10.3.8: icmp_seq=4 ttl=61 time=2.62 ms
64 bytes from 10.10.3.8: icmp_seq=5 ttl=61 time=2.77 ms
64 bytes from 10.10.3.8: icmp_seq=6 ttl=61 time=2.49 ms
```

Installing or Upgrading PICOS

This section details the procedure used to install Pica8 PICOS software.

- ONIE Version and BIOS/U-Boot Information of Verified Platforms
- Installing PICOS on Bare Metal Switches
- Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command
- Upgrading PICOS from Version 3.0 or Later Using Upgrade2
- Installing Debian Packages on PICOS
  - Installing GCC on PicOS
  - Installing Puppet on PicOS
  - Installing Salt on PicOS
- PICOS Installation and Upgrade Guide for FS S5810 Series, S3410 Series, S5860 Series and N8560-32C Switches
  - Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Console Port)
  - Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Console Port)
  - Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches
  - Installing PICOS for FS S3410 Series Switches
  - Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Eth0 or Inband Management Interface)
  - Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Eth0 or Inband Management Interface)
- PICOS Debian Package Upgrade User Guide

ONIE Version and BIOS/U-Boot Information of Verified Platforms

The ONIE and BIOS/U-Boot Version information of platforms verified in the lab are listed below. The users can find the ONIE version information in the **onie-syseeprom** command output.

Platform	BIOS/U-Boot Version	ONIE Version
AS4610_54P	none	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 159 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 15 4610-54P-O-AC-F Part Number 0x22 13 FP1ZZ5654001A Serial Number 0x23 12 EC1731000333 Base MAC Address 0x24 6 A8:2B:B5:70:43:40 Manufacture Date 0x25 19 08/22/2017 19:30:27 Label Revision 0x27 3 R01 Platform Name 0x28 23 arm-accton_as4610_54-r0 ONIE Version 0x29 13 2016.05.00.04 MAC Addresses 0x2A 2 55 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 5 001.9 CRC-32 0xFE 4 0xDABC2397 Checksum is valid.
AS4610_54T	none	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 159 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 15 4610-54T-O-AC-F Part Number 0x22 13 F0PEC4654000Z Serial Number 0x23 12 EC1741001625 Base MAC Address 0x24 6 A8:2B:B5:CD:6C:C0 Manufacture Date 0x25 19 10/30/2017 12:56:49 Label Revision 0x27 3 R01 Platform Name 0x28 23 arm-accton_as4610_54-r0 ONIE Version 0x29 13 2016.05.00.04 MAC Addresses 0x2A 2 55 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 5 001.9 CRC-32 0xFE 4 0xF40F7512 Checksum is valid.
AS4610_54T_B	none	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 159 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 15 4610-54T-O-AC-B Part Number 0x22 13 F0PEC4654003Z Serial Number 0x23 12 EC1631000053 Base MAC Address 0x24 6

		C4:39:3A:FF:2D:C0 Manufacture Date 0x25 19 08/05/2016 11:45:43 Label Revision 0x27 3 R0A MAC Addresses 0x2A 2 55 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 5 001.7 Platform Name 0x28 23 arm-accton_as4610_54-r0 ONIE Version 0x29 13 2018.02.00.03 CRC-32 0xFE 4 0x9DC28EDF Checksum is valid.
AS4610_30P	none	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 160 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 15 4610-30P-O-AC-F Part Number 0x22 13 F0PEC4630402Z Serial Number 0x23 12 EC1815000436 Base MAC Address 0x24 6 3C:2C:99:89:89:00 Manufacture Date 0x25 19 04/15/2018 23:45:48 Label Revision 0x27 4 R01A Platform Name 0x28 23 arm-accton_as4610_30-r0 ONIE Version 0x29 13 2016.05.00.04 MAC Addresses 0x2A 2 31 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 5 001.9 CRC-32 0xFE 4 0xCD54AF53 Checksum is valid.
AS4610_30T	none	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 160 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 15 4610-30T-O-AC-F Part Number 0x22 13 F0PEC4630001Z Serial Number 0x23 12 EC1806001291 Base MAC Address 0x24 6 3C:2C:99:41:47:E0 Manufacture Date 0x25 19 02/12/2018 23:08:49 Label Revision 0x27 4 R01A Platform Name 0x28 23 arm-accton_as4610_30-r0 ONIE Version 0x29 13 2016.05.00.04 MAC Addresses 0x2A 2 31 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 5 001.9 CRC-32 0xFE 4 0x4FF5BAD3 Checksum is valid.
S4048-ON	Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc. BIOS Date: 02/22/2017 02:29:52 Ver: 0ACBZ018	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 149 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 7 S4048ON Part Number 0x22 6 099TJK Serial Number 0x23 20 CN099TJK282985640054 Base MAC Address 0x24 6

		34:17:EB:FA:90:C4 Manufacture Date 0x25 19 06/08/2015 20:36:30 Label Revision 0x27 3 A00 MAC Addresses 0x2A 2 256 Manufacturer 0x2B 5 28298 Country Code 0x2C 2 CN Service Tag 0x2F 7 FX4PX42 Vendor Extension 0xFD 6 0x36 0x37 0x34 0x2D 0x46 0x46 Platform Name 0x28 26 x86_64-dell_s4000_c2338-r0 Loader Version 0x29 8 3.21.1.1 CRC-32 0xFE 4 0x7EB3C763 Checksum is valid.
S4128F-ON	Version 2.17.1245. Copyright (C) 2017 American Megatrends, Inc. BIOS Date: 04/26/2017 04:20:58 Ver: 0ACBZ028	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 180 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 9 S4128F-ON Part Number 0x22 6 02NK09 Serial Number 0x23 20 CN02NK092829886J0109 Base MAC Address 0x24 6 E4:F0:04:DF:67:16 Manufacture Date 0x25 19 06/19/2018 11:32:52 Device Version 0x26 1 1 Label Revision 0x27 3 A02 Platform Name 0x28 30 x86_64-dellemc_s4128f_c2338-r0 ONIE Version 0x29 10 3.33.1.1-4 MAC Addresses 0x2A 2 128 Manufacturer 0x2B 5 28298 Country Code 0x2C 2 CN Vendor Name 0x2D 8 Dell EMC Diag Version 0x2E 10 3.33.3.0-1 Service Tag 0x2F 7 HPPKXC2 Vendor Extension 0xFD 4 0x00 0x00 0x02 0xA2 CRC-32 0xFE 4 0x1A25266A Checksum is valid.
S4148T-ON	Version 2.17.1245. Copyright (C) 2017 American Megatrends, Inc. BIOS Date: 07/06/2017 01:44:00 Ver: 0ACBZ028	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 180 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 9 S4148T-ON Part Number 0x22 6 0JD8R7 Serial Number 0x23 20 CN0JD8R7282987CN0053 Base MAC Address 0x24 6 E4:F0:04:80:EA:CC Manufacture Date 0x25 19 12/23/2017 16:32:17 Device Version 0x26 1 1 Label Revision 0x27 3 A01 MAC Addresses 0x2A 2 256 Manufacturer 0x2B 5 28298 Country Code 0x2C 2 CN Vendor Name 0x2D 8 Dell EMC Service Tag 0x2F 7 6SCCXC2 Vendor Extension 0xFD 4 0x00 0x00 0x02 0xA2 Platform Name 0x28 30 x86_64-dellemc_s4148t_c2338-r0 ONIE Version 0x29 10 3.33.1.1-6 Diag Version 0x2E 10 3.33.3.1-6 CRC-32 0xFE 4 0xD89AF6DE Checksum is valid.
S4148F-ON	Version 2.17.1245. Copyright (C) 2017 American Megatrends, Inc. BIOS Date: 12/04/2017 20:42:30 Ver: 0ACBZ028	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 179 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 9 S4148F-ON Part Number 0x22 6 0R2RKC Serial Number 0x23 20

		TW0R2RKC2829872D0046 Base MAC Address 0x24 6 14:18:77:18:2C:B8 Manufacture Date 0x25 19 02/13/2017 19:32:31 Device Version 0x26 1 1 Label Revision 0x27 3 X01 MAC Addresses 0x2A 2 256 Manufacturer 0x2B 5 28298 Country Code 0x2C 2 TW Vendor Name 0x2D 8 DELL EMC Service Tag 0x2F 7 CM31XC2 Vendor Extension 0xFD 4 0x00 0x00 0x02 0xA2 Platform Name 0x28 29 x86_64-dellemc_s4100_c2338-r0 ONIE Version 0x29 10 3.33.1.1-4 Diag Version 0x2E 10 3.33.3.0-1 CRC-32 0xFE 4 0x42273778 Checksum is valid.
AS7712_32X	Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc. BIOS Date: 09/08/2015 11:15:24 Ver:	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 168 TLV Name Code Len Value ---------- ---- --- ----- Manufacture Date 0x25 19 10/28/2015 20:33:51 Label Revision 0x27 4 R0AB Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Base MAC Address 0x24 6 CC:37:AB:63:8B:84 Serial Number 0x23 14 771232X1541003 Part Number 0x22 13 FP3ZZ7632014A Product Name 0x21 15 7712-32X-O-AC-F MAC Addresses 0x2A 2 131 Vendor Name 0x2D 8 Edgecore Diag Version 0x2E 7 0.0.5.4 Platform Name 0x28 27 x86_64-accton_as7712_32x-r0 ONIE Version 0x29 13 2018.11.00.02 CRC-32 0xFE 4 0x9208666A Checksum is valid.
Z9100-ON	Version 2.17.1245. Copyright (C) 2017 American Megatrends, Inc. BIOS Date: 02/22/2017 21:20:05 Ver: 0ACBZ028	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 168 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 8 Z9100-ON Part Number 0x22 6 04HW8N Serial Number 0x23 20 CN04HW8N7793163I0010 Base MAC Address 0x24 6 4C:76:25:E8:D7:C0 Manufacture Date 0x25 19 03/19/2016 12:39:24 Device Version 0x26 1 1 Label Revision 0x27 3 A00 Platform Name 0x28 26 x86_64-dell_z9100_c2538-r0 ONIE Version 0x29 8 3.23.1.3 MAC Addresses 0x2A 2 384 Manufacturer 0x2B 5 77931 Country Code 0x2C 2 CN Vendor Name 0x2D 4 DELL Diag Version 0x2E 6 01_010 Service Tag 0x2F 7 2QWRG02 Vendor Extension 0xFD 7 0x00 0x00 0x02 0xA2 0x2D 0x46 0x46 CRC-32 0xFE 4 0x3B190E49 Checksum is valid.
AS7816_64X	Version 2.19.1269. Copyright (C) 2018 American Megatrends, Inc. BIOS Date: 10/05/2018	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 171 TLV Name Code Len Value

	08:57:44 Ver: AS7816-64X V36 20181004	---------- ---- --- ----- Manufacture Date 0x25 19 11/02/2018 16:32:21 Label Revision 0x27 4 R01A Platform Name 0x28 27 x86_64-accton_as7816_64x-r0 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Product Name 0x21 17 7816-64X-O-AC-F-R Part Number 0x22 13 FP3ZZ7664020A Serial Number 0x23 14 781664X1843004 Base MAC Address 0x24 6 B8:6A:97:73:6A:3E MAC Addresses 0x2A 2 300 ONIE Version 0x29 13 2018.11.00.02 Diag Version 0x2E 8 0.1.0.17 CRC-32 0xFE 4 0x84DD5474 Checksum is valid.
Z9264F-ON	Version 2.19.1266. Copyright (C) 2018 American Megatrends, Inc. BIOS Date: 09/17/2018 21:25:57 Ver: 0ACHI032	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 181 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 9 Z9264F-ON Part Number 0x22 6 0RWYT4 Serial Number 0x23 20 CN0RWYT4DND008660010 Base MAC Address 0x24 6 20:04:0F:05:D4:97 Manufacture Date 0x25 19 06/06/2018 03:00:21 Device Version 0x26 1 1 Label Revision 0x27 3 A00 Platform Name 0x28 30 x86_64-dellemc_z9264f_c3538-r0 ONIE Version 0x29 10 3.42.1.9-3 MAC Addresses 0x2A 2 640 Manufacturer 0x2B 5 DND00 Country Code 0x2C 2 CN Vendor Name 0x2D 8 Dell EMC Diag Version 0x2E 11 3.00.3.41-1 Service Tag 0x2F 7 20GKXC2 Vendor Extension 0xFD 4 0x00 0x00 0x02 0xA2 CRC-32 0xFE 4 0xD8EFCB81 Checksum is valid. ONIE:/ #
AS5812_54T	Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc. BIOS Date: 08/20/2015 10:55:33 Ver: A02 0820	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 168 TLV Name Code Len Value ---------- ---- --- ----- Manufacture Date 0x25 19 08/11/2016 16:36:46 Diag Version 0x2E 7 1.0.0.5 Label Revision 0x27 4 R01A Platform Name 0x28 27 x86_64-accton_as5812_54t-r0 ONIE Version 0x29 13 2015.11.00.01 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Base MAC Address 0x24 6 C4:39:3A:FB:BF:6C Serial Number 0x23 14 581254T1631023 Part Number 0x22 13 FP1ZZ5654031A Product Name 0x21 15 5812-54T-O-AC-F MAC Addresses 0x2A 2 74 Vendor Name 0x2D 8 Edgecore CRC-32 0xFE 4 0xCBA5E40E Checksum is valid.
HPE AL 6921-54X	Version 2.16.1242. Copyright (C) 2013	ONIE:/ # onie-syseeprom TlvInfo Header:

	American Megatrends, Inc. BIOS Date: 08/20/2015 10:55:33 Ver:	Id String: TlvInfo Version: 1 Total Length: 231 TLV Name Code Len Value ---------- ---- --- ----- Manufacture Date 0x25 19 05/24/2016 14:49:30 Diag Version 0x2E 7 1.0.0.3 Label Revision 0x27 4 R01A Platform Name 0x28 27 x86_64-accton_as5812_54x-r0 ONIE Version 0x29 13 2015.11.00.01 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Base MAC Address 0x24 6 E0:07:1B:CB:20:50 Serial Number 0x23 10 TW65JQH009 Part Number 0x22 13 F0P8J5654000A Product Name 0x21 64 HPE Altoline 6921 48SFP+ 6QSFP+ x86 ONIE AC Front-to-Back Switch MAC Addresses 0x2A 2 74 Vendor Name 0x2D 26 Hewlett Packard Enterprise CRC-32 0xFE 4 0xADE27C84 Checksum is valid.
AS5712_54X	Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc. BIOS Date: 11/20/2014 10:55:31 Ver:	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 167 TLV Name Code Len Value ---------- ---- --- ----- Manufacture Date 0x25 19 12/18/2014 11:22:02 Diag Version 0x2E 7 2.0.0.7 MAC Addresses 0x2A 2 74 Manufacturer 0x2B 6 Accton Country Code 0x2C 2 TW Vendor Name 0x2D 8 Edgecore Base MAC Address 0x24 6 70:72:CF:B7:65:44 Part Number 0x22 13 FP1ZZ5654001A Serial Number 0x23 14 571254X1419017 Label Revision 0x27 3 R0A Product Name 0x21 15 5712-54X-O-AC-F Platform Name 0x28 27 x86_64-accton_as5712_54x-r0 ONIE Version 0x29 13 2015.11.00.05 CRC-32 0xFE 4 0x37B6E65B Checksum is valid.
N3248PXE-ON	Version 2.19.1266. Copyright (C) 2019 American Megatrends, Inc. BIOS Date: 06/18/2019 23:21:39 Ver: 0ACHI040	ONIE:/ # onie-syseeprom TlvInfo Header: Id String: TlvInfo Version: 1 Total Length: 186 TLV Name Code Len Value ---------- ---- --- ----- Product Name 0x21 11 N3248PXE-ON Part Number 0x22 6 0WYGRV Serial Number 0x23 20 TW0WYGRVDNT0097I0012 Base MAC Address 0x24 6 50:9A:4C:E6:7B:70 Manufacture Date 0x25 19 07/18/2019 17:41:23 Device Version 0x26 1 1 Label Revision 0x27 4 X01A Platform Name 0x28 32 x86_64-dellemc_n3248pxe_c3338-r0 ONIE Version 0x29 10 3.45.1.9-4 MAC Addresses 0x2A 2 128 Manufacturer 0x2B 5 DNT00 Country Code 0x2C 2 TW Vendor Name 0x2D 8 Dell EMC Diag Version 0x2E 11 3.00.3.41-2 Service Tag 0x2F 7 37QFXC2

Installing PICOS on Bare Metal Switches

- Introduction
- Installation Notes and Tools
  - What is ONIE
- Traditional Installation
  - Mind Map of Installation Process
  - Manual Installation Process
  - Automatic Installation Process
- Nos-boot-mode Installation
  - Manual Installation Process
  - Automated Installation Process
- Verifying Version after Installation
- Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X
  - Check Label Revision
  - Solution

Introduction

When using ONIE installer to install PICOS, the installer reinstalls the software, rebuilds all the PICOS file system. This can erase the configuration files and system logs from the previous installation.

After a successful ONIE installation of PICOS 4.x, the system generates multiple system partitions including PicOS (partition size: 2G), PicOS2 (partition size: 2G) and User-Data partitions. Among them, PicOS and PicOS2 are two independent system boot partitions. One of them is the active partition on which the running system resides, and the other is the inactive partition. The two-system-boot-partition feature allows the system to revert to a previous version of the installed software package when the it fails to upgrade PICOS by using upgrade2 command.

The ONIE installer removes all partitions to rebuild a brand new OS only when there is no User-Data partition. However, if there exists a User-Data partition (for example, install a new version 4.0.1 from the old one 4.0.0), the ONIE installer only rewrites the "PicOS" partition, installs the new installation package to this partition and sets the system on "PicOS" partition as the default and sole boot system.

User-Data partition is a reserved partition which is not affected by ONIE installer and upgrade unless user manually removes it. User-Data partition uses all the available space left on the disk. Users can use this partition to store files and data.

This document describes how to install PICOS 4.x software using ONIE installer.

Installation Notes and Tools

The installation methods used to install a new PICOS are traditional installation and nos-boot-mode installation. You can choose a suitable installation method that is convenient and appropriate for your installation environment.

- If you want to install PICOS through a console port, refer to sections Traditional Installation or Nos-boot-mode Installation.
- If you want to install the PICOS through a non-console port (through the management port), refer to section Nos-boot-mode Installation.

- You need to log in through the console port of the switch and perform the ONIE installation.
- Other NOSes including user data will be removed when install PICOS under ONIE environment.
- When the ONIE installer is used to downgrade the PICOS version from version 4.x to PICOS 3.x or lower versions, we first need to use ONIE to uninstall the higher version PICOS before proceeding with installing PICOS 3.x or a lower version. On the ARM platform, execute the **onie_uninstaller** command at the ONIE prompt to uninstall the current version PICOS. On the x86 platform, select the "**ONIE: Uninstall OS**" option in the GRUB menu to uninstall the current version PICOS.
- If you enter GRUB rescue mode and the switch has GPT format partition, you can use the following commands to reset the GRUB boot variable to enter ONIE GRUB and then install PICOS.

  ```
  grub rescue> set prefix=(hd0,gpt2)/grub
  grub rescue> set root=(hd0,gpt2)
  grub rescue> insmod normal
  grub rescue> normal
  ```

- Do not plug in the USB disk during onie-nos-installer process until ONIE starts up. If you have plugged in the USB disk before the installation operation, ONIE will find the installer on the USB disk when beginning the installation. On AS4610 series switches, when installation is complete, the installer will display: **Please take out the usb disc**, then remove the USB disk within 10 seconds after installation successful, and before machine restarts.
- All X86 platforms share one installation and upgrade package with the name fixed as: **onie-installer-picos-VERSION-x86.bin**, where **VERSION** is the release version. X86 platform are listed below:
  - FS N9550-32D
  - FS N8550-64C
  - FS N5850-48S6Q
  - FS N8550-48B8C
  - FS N8550-32C
  - FS N8560-64C
  - FS N8550-24CD8D
  - FS N9600-64OD
  - Edgecore AS4630-54PE
  - Edgecore AS5712-54X
  - Edgecore AS5812-54T
  - Edgecore AS5812-54X
  - Edgecore AS7312-54X

- Edgecore AS7326-56X
- Edgecore AS7712-32X
- Edgecore AS7726-32X
- Edgecore AS7816-64X
- Edgecore AS5835-54X
- Edgecore AS9716-32D
- DELL N3248P-ON
- DELL N3248PXE-ON
- DELL N3224PX-ON
- DELL N3248X-ON
- DELL S4048-ON
- DELL S4148F-ON
- DELL S4148T-ON
- DELL S4128F-ON
- DELL S5224F-ON
- DELL S5296F-ON
- DELL S5212F-ON
- DELL S5248F-ON
- DELL Z9100-ON
- DELL Z9264F-ON
- DELL N3224T-ON
- DELL S4128T-ON

What is ONIE

ONIE (Open Network Install Environment) is an open source project of OCP (Open Compute Project). ONIE provides the environment to install any network operating system on a bare metal network switch. ONIE liberates users from captive pre-installed network operating systems, like the Cisco IOS, and provides them with a choice.

ONIE is a small Linux operating system that comes pre-installed as firmware on bare metal network switches. ONIE acts as an enhanced boot loader, extending the features provided by U-Boot. ONIE is used to install Pica8 PICOS on compatible switches. The bare metal switches listed in the PICOS Hardware Compatibility List must be pre-loaded with ONIE prior to installing PICOS.

Traditional Installation

NOTE :

- You need to log in through the console port of the switch and perform the ONIE installation described in this section.
- The installation method described in this section only applies to platforms that have pre-installed ONIE.

Mind Map of Installation Process

Figure1 shows the mind map of PICOS installation process.

Figure1 Mind Map of PICOS installation process

Manual Installation Process

The following example describes the installation of PICOS via manual installation method.

Step1 Make sure that the installation package of **.bin** file has been load to the server (server could be HTTP, TFTP, or an FTP server or the switch local directory depending on the actual installation environment).

Step2 Enter ONIE installation environment. The process is different on the following two types of platforms:

- **ARM Platforms (AS4610 Series Switches)**
- **x86 Platform**

- **ARM Platforms (AS4610 Series Switches)**

a) Verify that the switch is pre-loaded with ONIE, which will be used to load PICOS on the switch. Power on the switch and interrupt the boot sequence by pressing any key when the following line is shown:

```
Hit any key to stop autoboot:
```

b) User will then reach the U-Boot command prompt indicated by ->. Run the **printenv** command at the U-Boot prompt. If the information displayed contains keywords like **onie_initargs** and **onie_machine**, the switch is pre-loaded with ONIE.

```
LOADER->printenv
active=image1
autoload=no
baudrate=115200
bootcmd=run check_boot_reason;run PicOS_bootcmd;run onie_bootcmd
bootdelay=10
check_boot_reason=if test -n $onie_boot_reason; then setenv onie_bootargs boot_reason=$onie_boot_reason; run onie_b
consoledev=ttyS0
dhcp_user-class=arm-accton_as4610_54-r0_uboot
dhcp_vendor-class-identifier=arm-accton_as4610_54-r0
ethact=eth-0
ethaddr=00:18:23:30:E7:8F
fdtaddr=0xc00000
fpboot=setenv bootargs console=${consoledev},${baudrate} maxcpus=2 mem=1024M root=/dev/ram ${mtdparts} ubi.mtd=4 et
gatewayip=192.168.0.1
initrd_high=0x80000000
ipaddr=192.168.0.1
loadaddr=0x70000000
loads_echo=1
mfg=mfg
mfgdiags=run fpboot ; nand read ${loadaddr} diags ; bootm ${loadaddr}
mfgdiags_recovery=nand read ${loadaddr} diags2 ; nand erase.part diags ; nand write ${loadaddr} diags
mtdids=nand0=nand_iproc.0
mtdparts=mtdparts=nand_iproc.0:1m(uboot),2m(shmoo),1m(nenv),12m(onie),3992m(open),12m(onie2),2m(vpd),6m(sys_eeprom)
netmask=255.255.255.0
nos_bootcmd=true
onie_args=run onie_initargs onie_platformargs
onie_bootcmd=echo Loading Open Network Install Environment ...; echo Platform: $onie_platform ; echo Version : $oni
onie_dropbear_dss_host_key=begin-base64@600@d#AAAAB3NzaC1kc3MAAACBAIN7HOS7UGtQ+RS9R5Rdim9s4iadCBQ9SEFnHJZ2#ulK15hNZ
onie_dropbear_rsa_host_key=begin-base64@600@r#AAAAB3NzaC1yc2EAAAADAQABAAAAgQCMTqwNhnJpuSLYAdRA/jjm1lyBaJF1#ovs3Hp0(
onie_initargs=setenv bootargs quiet console=$consoledev,$baudrate
onie_machine=accton_as4610_54
onie_machine_rev=0
onie_platform=arm-accton_as4610_54-r0
onie_platformargs=setenv bootargs $bootargs serial_num=${serial#} ${platformargs} eth_addr=$ethaddr $onie_bootargs
onie_recovery=nand read ${loadaddr} onie2 ; nand erase.part onie ; nand write ${loadaddr} onie
onie_rescue=setenv onie_boot_reason rescue && boot
onie_start=onie
onie_sz.b=0x00c00000
onie_uninstall=setenv onie_boot_reason uninstall && boot
onie_update=setenv onie_boot_reason update && boot
onie_vendor_id=27658
onie_version=master-201603091701-dirty
PicOS_bootcmd=usb start;run platformargs;setenv bootargs root=/dev/sda1 rw noinitrd console=$consoledev,$baudrate r
platform=accton_as4610_54
platformargs=mtdparts=nand_iproc.0:1m(uboot),2m(shmoo),1m(nenv),12m(onie),3992m(open),12m(onie2),2m(vpd),6m(sys_eep
ramdiskaddr=0x3000000
serial#=A626P1DL174300014
serverip=192.168.0.10
stderr=serial
stdin=serial
stdout=serial
ubifscfg=ubi part nand0,4 0x0; ubifsmount fs
ver=U-Boot 2012.10-gcbef171 (Mar 09 2016 - 17:01:14) - ONIE master-201603091701-dirty

Environment size: 3992/65532 bytes
```

c) From U-Boot prompt, boot ONIE in rescue mode.

```
LOADER-> run onie_rescue
```

- **x86 Platform**

On x86 platform, it uses GRUB menu to install OS via ONIE.

a) Reboot the system, and enter **ONIE** installation environment from the GRUB menu:

```
+----------------------------------------------------------------------------+
| PicOS                                                                      |
|*ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

b) From GRUB prompt, choose **ONIE: Rescue** to Install OS, boot ONIE in rescue mode.

```
                         GNU GRUB  version 2.02~beta2+e4a1fe391
+----------------------------------------------------------------------------+
|*ONIE: Install OS                                                           |
| ONIE: Rescue                                                               |
| ONIE: Uninstall OS                                                         |
| ONIE: Update ONIE                                                          |
| ONIE: Embed ONIE                                                           |
| DIAG: Accton Diagnostic                                                    |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
```

Step3 Run **onie-nos-install** command as follows to manually install PICOS.

- **Install via TFTP**

```
ONIE# onie-nos-install tftp://<path to image>/PICOS.bin
```

- **Install via FTP**

When installing via FTP, you need to type **username** and **password** of the FTP server on which the image file is loaded.

```
ONIE# onie-nos-install ftp://username:password@<path to image>/PICOS.bin
```

- **Install via HTTP**

```
ONIE# onie-nos-install http://<path to image>/PICOS.bin
```

- **Install from Local Directory**

a) In **ONIE rescue** mode, copy the image file to the current directory.

```
ONIE# scp username@<path to image>/PICOS.bin .
```

b) Run **onie-nos-install** command to start installation.

```
ONIE# onie-nos-install PICOS.bin
```

For example,

```
ONIE:/ # onie-nos-install onie-installer-picos-4.0.0-8b1219e112-x86.bin
discover: Rescue mode detected. No discover stopped.
ONIE: Executing installer: onie-installer-picos-4.0.0-8b1219e112-x86.bin
Verifying image checksum ... OK.
Preparing image archive ... OK.
  [1]  PICOS L2/L3 (default)
  [2]  PICOS Open vSwitch/OpenFlow
Enter your choice (1,2):1
PICOS L2/L3 is selected.
ONIE installation will overwrite the configuration file of existing system.
It is recommended to follow the upgrade procedure to upgrade the system.
Press any key to stop the installation...
10 9 8 7 6 5 4 3 2 1 ...
```

The installer runs automatically, before start installation, it will prompt to choose the option to make PICOS to boot into L2/L3 or OVS mode. If not selected, then PICOS boots into L2/L3.

After finishing installation, the device reboots automatically, the system then comes up running the new network operating system.

NOTE :

- After the system restarts, you need to enter the username and password, the initial login username is **admin** and password is **pica8**.
- After the username and password are entered, user will be asked to choose a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Automatic Installation Process

The automatic installation process uses the DHCP message exchange process to download and install software packages.

Step1 Make sure the switch is connected to DHCP and HTTP servers and the PICOS installation software package is downloaded to the HTTP server.

a) DHCP server configuration: define the path of the installation package and then start DHCP server service:

```
host pica8-3922 {
hardware ethernet 70:72:cf:12:34:56;
fixed-address 192.168.2.50;
option default-url = "http://192.168.2.42/onie-installer-picos-4.0.0-8b1219e112-x86.bin";
}
```

b) Check if the **.bin** installation file is loaded onto the HTTP server:

```
root@dev:/var/www# ls
index.html onie-installer-powerpc.bin
```

Step2 Install PICOS via ONIE. The process is different on the following two types of platforms:

- **ARM Platforms (AS4610 Series Switches)**
- **x86 Platform**

- **ARM Platforms (AS4610 Series Switches)**

a) Verify that the switch is pre-loaded with ONIE, which will be used to load PICOS on the switch. Power on the switch and interrupt the boot sequence by pressing any key when the following line is shown:

```
Hit any key to stop autoboot:
```

b) User will then reach the U-Boot command prompt indicated by ->. Run the **printenv** command at the U-Boot prompt. If the information displayed contains keywords like **onie_initargs** and **onie_machine**, the switch is pre-loaded with ONIE.

```
LOADER-> printenv
active=image1
autoload=no
baudrate=115200
bootcmd=run check_boot_reason;run PicOS_bootcmd;run onie_bootcmd
bootdelay=10
check_boot_reason=if test -n $onie_boot_reason; then setenv onie_bootargs boot_reason=$onie_boot_reason; run onie_b
consoledev=ttyS0
dhcp_user-class=arm-accton_as4610_54-r0_uboot
dhcp_vendor-class-identifier=arm-accton_as4610_54-r0
ethact=eth-0
ethaddr=00:18:23:30:E7:8F
```

```
fdtaddr=0xc00000
fpboot=setenv bootargs console=${consoledev},${baudrate} maxcpus=2 mem=1024M root=/dev/ram ${mtdparts} ubi.mtd=4 e
gatewayip=192.168.0.1
initrd_high=0x80000000
ipaddr=192.168.0.1
loadaddr=0x70000000
loads_echo=1
mfg=mfg
mfgdiags=run fpboot ; nand read ${loadaddr} diags ; bootm ${loadaddr}
mfgdiags_recovery=nand read ${loadaddr} diags2 ; nand erase.part diags ; nand write ${loadaddr} diags
mtdids=nand0=nand_iproc.0
mtdparts=mtdparts=nand_iproc.0:1m(uboot),2m(shmoo),1m(nenv),12m(onie),3992m(open),12m(onie2),2m(vpd),6m(sys_eeprom)
netmask=255.255.255.0
nos_bootcmd=true
onie_args=run onie_initargs onie_platformargs
onie_bootcmd=echo Loading Open Network Install Environment ...; echo Platform: $onie_platform ; echo Version : $on
onie_dropbear_dss_host_key=begin-base64@600@d#AAAAB3NzaC1kc3MAAACBAIN7HOS7UGtQ+RS9R5Rdim9s4iadCBQ9SEFnHJZ2#ulK15hN
onie_dropbear_rsa_host_key=begin-base64@600@r#AAAAB3NzaC1yc2EAAAADAQABAAAAgQCMTqwNhnJpuSLYAdRA/jjm1lyBaJF1#ovs3Hp0
onie_initargs=setenv bootargs quiet console=$consoledev,$baudrate
onie_machine=accton_as4610_54
onie_machine_rev=0
onie_platform=arm-accton_as4610_54-r0
onie_platformargs=setenv bootargs $bootargs serial_num=${serial#} ${platformargs} eth_addr=$ethaddr $onie_bootargs
onie_recovery=nand read ${loadaddr} onie2 ; nand erase.part onie ; nand write ${loadaddr} onie
onie_rescue=setenv onie_boot_reason rescue && boot
onie_start=onie
onie_sz.b=0x00c00000
onie_uninstall=setenv onie_boot_reason uninstall && boot
onie_update=setenv onie_boot_reason update && boot
onie_vendor_id=27658
onie_version=master-201603091701-dirty
PicOS_bootcmd=usb start;run platformargs;setenv bootargs root=/dev/sda1 rw noinitrd console=$consoledev,$baudrate
platform=accton_as4610_54
platformargs=mtdparts=nand_iproc.0:1m(uboot),2m(shmoo),1m(nenv),12m(onie),3992m(open),12m(onie2),2m(vpd),6m(sys_ee
ramdiskaddr=0x3000000
serial#=A626P1DL174300014
serverip=192.168.0.10
stderr=serial
stdin=serial
stdout=serial
ubifscfg=ubi part nand0,4 0x0; ubifsmount fs
ver=U-Boot 2012.10-gcbef171 (Mar 09 2016 - 17:01:14) - ONIE master-201603091701-dirty

Environment size: 3992/65532 bytes
```

c) Input command **run onie_bootcmd**, which will automatically install PICOS on the switch.

```
LOADER -> run onie_bootcmd
Loading Open Network Install Environment ...
Platform: arm-accton_as4610_54-r0
Version : 2021.09.00.03
WARNING: adjusting available memory to 30000000
## Booting kernel from Legacy Image at 02000000 ...
Image Name: as4610_54x.1.6.1.3
Image Type: ARM Linux Multi-File Image (gzip compressed)
Data Size: 3514311 Bytes = 3.4 MiB
Load Address: 00000000
Entry Point: 00000000
Contents:
Image 0: 2762367 Bytes = 2.6 MiB
Image 1: 733576 Bytes = 716.4 KiB
Image 2: 18351 Bytes = 17.9 KiB
Verifying Checksum ... OK
## Loading init Ramdisk from multi component Legacy Image at 02000000 ...
## Flattened Device Tree from multi component Image at 02000000
Booting using the fdt at 0x02355858
Uncompressing Multi-File Image ... OK
Loading Ramdisk to 2ff4c000, end 2ffff188 ... OK
Loading Device Tree to 03ff8000, end 03fff7ae ... OK
Cannot reserve gpages without hugetlb enabled
```

```
setup_arch: bootmem
as4610_54x_setup_arch()
arch: exit

pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
sd 0:0:0:0: [sda] No Caching mode page present
sd 0:0:0:0: [sda] Assuming drive cache: write through
sd 0:0:0:0: [sda] No Caching mode page present
sd 0:0:0:0: [sda] Assuming drive cache: write through
sd 0:0:0:0: [sda] No Caching mode page present
sd 0:0:0:0: [sda] Assuming drive cache: write through
ONIE: Using DHCPv4 addr: eth0: 192.168.2.77 / 255.255.255.0
discover: installer mode detected. Running installer.
Please press Enter to activate this console. ONIE: Using DHCPv4 addr: eth0: 192.168.2.77 / 255.255.255.0
ONIE: Starting ONIE Service Discovery
ONIE: Executing installer: http://192.168.2.42/onie-installer-picos-4.0.0-8b1219e112-x86.bin
Verifying image checksum ... OK.
Preparing image archive ... OK.
PicOS installation
.........................................
./var/local/
./var/run
Setup PicOS environment ...
.........................................
XorPlus login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
admin@XorPlus$
```

- **x86 Platform**

On x86 platform, it uses GRUB menu to choose install OS via ONIE.

a) Reboot the system, and enter **ONIE** installation environment from the GRUB menu:

```
+----------------------------------------------------------------------------+
| PicOS                                                                      |
|*ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

b) From GRUB prompt, choose **ONIE: Rescue** to Install OS, boot ONIE in rescue mode.

```
                      GNU GRUB  version 2.02~beta2+e4a1fe391
+----------------------------------------------------------------------------+
|*ONIE: Install OS                                                           |
| ONIE: Rescue                                                               |
| ONIE: Uninstall OS                                                         |
| ONIE: Update ONIE                                                          |
| ONIE: Embed ONIE                                                           |
| DIAG: Accton Diagnostic                                                    |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
```

```
|                                                                              |
|                                                                              |
+------------------------------------------------------------------------------+
```

The installer runs and will reboot the system after installation is complete.

NOTE：

- After the system restarts, you need to enter the username and password, the initial login username is **admin** and password is **pica8**.
- After the username and password are entered, user will be asked to choose a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Nos-boot-mode Installation

NOTE：

- The installation method described in this section applies to installation through both the console port and the management port.
- The installation method described in this section only applies to platforms that have pre-installed ONIE.

The installation methods described in Traditional Installation must be performed through the console port. If you want to install the system through a non-console port, you can use the **nos-boot-mode** command to perform the installation which is described in this section.

Usage of **nos-boot-mode** command:

admin@Xorplus$sudo nos-boot-mode

USAGE

install or uninstall NOS(es)

SYNOPSIS

nos-boot-mode [install|uninstall]

DESCRIPTION

install- Install NOS

uninstall- Remove all NOS(es) including PICOS

When **nos-boot-mode install** command is executed, PICOS will switch to ONIE install mode, and the user should go on to complete the subsequent installation. The steps for the manual installation process and the automatic installation process using the **nos-boot-mode install** command are described below.

When **nos-boot-mode unsinstall** command is executed, the system will remove all NOS(es) including PICOS from the device. Therefore, it is suggested to use the **nos-boot-mode unsinstall** command with caution.

Manual Installation Process

Step1 Make sure that the installation package of **.bin** file has been loaded to the server (server could be HTTP, TFTP, or an FTP server or the switch local directory depending on the actual installation environment).

Step2 Execute the **nos-boot-mode install** command to enter ONIE installation environment.

```
admin@Xorplus:~$ sudo nos-boot-mode install
```

Step3 Type "**yes**" when the below prompt is shown, which will take the system will to ONIE install mode.

```
Type 'yes' to install NOS!
Type 'no' to exit
[no]/yes:
```

Step4 Run **onie-nos-install** command as follows to manually install PICOS.

- **Install via TFTP**

```
ONIE# onie-nos-install tftp://<path to image>/PICOS.bin
```

- **Install via FTP**

When installing via FTP, you need to type in the **username** and **password** for the FTP server on which the image file is loaded.

```
ONIE# onie-nos-install ftp://username:password@<path to image>/PICOS.bin
```

- **Install via HTTP**

```
ONIE# onie-nos-install http://<path to image>/PICOS.bin
```

- **Install from Local Directory**

a) In ONIE rescue mode, copy the image file to the current directory.

```
ONIE# scp username@<path to image>/PICOS.bin .
```

b) Run **onie-nos-install** command to start installation.

```
ONIE# onie-nos-install PICOS.bin
```

For example,

```
ONIE:/ # onie-nos-install onie-installer-picos-4.0.0-8b1219e112-x86.bin
discover: Rescue mode detected. No discover stopped.
ONIE: Executing installer: onie-installer-picos-4.0.0-8b1219e112-x86.bin
Verifying image checksum ... OK.
Preparing image archive ... OK.
  [1]  PICOS L2/L3 (default)
  [2]  PICOS Open vSwitch/OpenFlow
Enter your choice (1,2):1
PICOS L2/L3 is selected.
ONIE installation will overwrite the configuration file of existing system.
It is recommended to follow the upgrade procedure to upgrade the system.
Press any key to stop the installation...
10 9 8 7 6 5 4 3 2 1 ...
```

The installer runs automatically, before start installation, it will prompt to choose the option to make PICOS to boot into L2/L3 or OVS mode. If not selected, then PICOS boots into L2/L3.

After finishing installation, the device reboots automatically, the system then comes up running the new network operating system.

NOTE :

- After the system restarts, you need to enter the username and password, the initial login username is **admin** and password is **pica8**.
- After the username and password are entered, user will be asked to choose a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Automated Installation Process

The automatic installation process uses the DHCP message exchange process to download and install software packages.

Step1 Make sure the switch is connected to DHCP and HTTP servers, and the PICOS installation software package is downloaded to the HTTP server.

a) DHCP server configuration: define the path of the installation package and then start DHCP server service:

```
host pica8-3922 {
hardware ethernet 70:72:cf:12:34:56;
fixed-address 192.168.2.50;
option default-url = "http://192.168.2.42/onie-installer-picos-4.0.0-8b1219e112-x86.bin";
}
```

b) Check if the **.bin** installation file is loaded onto the HTTP server:

```
root@dev:/var/www# ls
index.html onie-installer-powerpc.bin
```

Step2 Execute the **nos-boot-mode install** command to enter ONIE installation environment.

```
admin@Xorplus$ sudo nos-boot-mode install
```

Step3 Type "**yes**" when the below prompt is shown, and the system will automatically complete the installation.

```
Type 'yes' to install NOS!
Type 'no' to exit
[no]/yes:
```

The installer runs automatically and will reboot the system after installation is completed.

NOTE :

- After the system restarts, you need to enter the username and password, the initial login username is **admin** and password is **pica8**.
- After the username and password are entered, user will be asked to choose a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Verifying Version after Installation

After system reboots automatically, the system will come up running the new network operating system.

```
admin@Xorplus> show version
Copyright (C) 2009-2022 Pica8, Inc.
===================================
Hardware Model                : as7312_54x
Linux System Version/Revision    : 4.0.0/8b1219e112
Linux System Released Date       : 5/18/2021
L2/L3 Version/Revision           : 4.0.0/8b1219e112
L2/L3 Released Date             : 5/18/2021
OVS/OF Version/Revision         : 4.0.0/8b1219e112
OVS/OF Released Date           : 5/18/2021
```

Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X

Installation or upgrade failure (for example, the switches cannot boot up after install) may occur on the old AS7326-56X hardware models (revision is R01F and before). When booting PICOS on AS7326-56X and detect hardware rev R01F, the system will log a warning message to prompt the hardware revision R01F is a pre-production hardware reversion: "This hardware revision R01F is a pre-production hardware rev, PICOS has applied a work around to work with PICOS. Support will be provided on a best effort basis".

To work around the issue, first we need to check the “Label Revision”. If it is an old hardware model (revision is R01F or before), then, we can perform the following provided solution after installation/upgrade to solve the problem.

Check Label Revision

Under ONIE prompt, run “**onie_syseeprom**” to get the “*Label Revision*”.

```
ONIE:/ # onie-syseeprom
TlvInfo Header:
   Id String:    TlvInfo
   Version:      1
   Total Length: 166
TLV Name             Code Len Value
-------------------- ---- --- -----
Manufacture Date     0x25  19 04/27/2019 02:10:06
Label Revision       0x27   4 R01B
Platform Name        0x28  27 x86_64-accton_as7326_56x-r0
ONIE Version         0x29  13 2018.05.00.05
Manufacturer         0x2B   6 Accton
Diag Version         0x2E   7 0.0.1.0
Base MAC Address     0x24   6 80:A2:35:81:D5:F0
Serial Number        0x23  14 732656X1916012
Country Code         0x2C   2 TW
Part Number          0x22  13 FP4ZZ7656005A
Product Name         0x21  15 7326-56X-O-AC-F
MAC Addresses        0x2A   2 256
Vendor Name          0x2D   6 Accton
CRC-32               0xFE   4 0xC3D3F2DE
Checksum is valid.
ONIE:/ #
```

Solution

You can follow the steps below after installation/upgrade, to fix the problem of installation and upgrade failure on the old AS7326-56X hardware model (revision R01F or before).

Step1 Power cycle the switch.

Step2 From the GRUB menu, choose “**ONIE”** to enter ONIE GRUB menu:

```
+----------------------------------------------------------------------------+
| PicOS                                                                      |
|*ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
```

```
|                                                                              |
|                                                                              |
|                                                                              |
+------------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Step3 From ONIE GRUB menu, choose "**ONIE: Rescue"** to launch ONIE in Rescue mode.

```
                         GNU GRUB  version 2.02~beta2+e4a1fe391
+------------------------------------------------------------------------------+
| ONIE: Install OS                                                             |
|*ONIE: Rescue                                                                 |
| ONIE: Uninstall OS                                                           |
| ONIE: Update ONIE                                                            |
| ONIE: Embed ONIE                                                             |
| DIAG: Accton Diagnostic                                                      |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
+------------------------------------------------------------------------------+
```

Step4 Press Enter to display the ONIE prompt.

Step5 Mount PicOS partition with label is "PicOS".

```
ONIE:/ # blkid
/dev/sda7: LABEL="User-Data" UUID="be63cef8-4560-4c48-ab5a-8f7ced5a950b"
/dev/sda6: LABEL="PicOS2" UUID="f589e53f-4cd1-44ba-8384-f339f4e2b2ac"
/dev/sda5: LABEL="PicOS" UUID="8ca5f7ed-5a15-4a2a-944c-4d8872647bf5"
/dev/sda4: LABEL="PICOS-GRUB" UUID="782a1372-4b66-4783-b920-dab1df8ec6e4"
/dev/sda3: LABEL="ACCTON-DIAG" UUID="3e4117d0-1926-472a-9d9e-08883df83d40"
/dev/sda2: LABEL="ONIE-BOOT" UUID="1a90abd8-f065-4f7a-90a0-af122b8805fa"
ONIE:/ #
ONIE:/ # mount /dev/sda5 /mnt
```

Step6 Execute the following command to modify the I2C access address.

```
ONIE:/ # sed -I "s/0x57/0x56/" /mnt/etc/rc_hw.sh
ONIE:/ # sync
```

Step7 Unmount the PicOS partition.

```
ONIE:/ # unmount /dev/sda5
```

Step8 Reboot the switch.

```
ONIE:/ # reboot
```

Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command

- Partitioning
- Supported Platforms
- Preparation before Upgrading
  - Checking the Running PicOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data in Flash
  - Checking the Available Flash Space
- Upgrading Notes
- Usage of Upgrade Command
  - Usage of Backup-file=(*.lst) Option
- Upgrading Procedure
- Verifying Version after Upgrading
- Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X
  - Check Label Revision
  - Solution

NOTE:

- This document ONLY applies to upgrade from version 4.0.0 or the later version using the **upgrade** command. If you want to upgrade PICOS from the version before 4.0.0, use ONIE installation process described in Installing PICOS on Bare Metal Switches.
- This upgrading guide is not available for FS S5810 Series and S5860 Series switches.
- N8560-32C uses the ONIE method for upgrade described in this guide, while the installation uses Rboot method, please refer to Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches for details on the installation process.
- The installation package name for N8560-32C includes the suffix '**-rboot**', for example, **N8560_picos-4.4.5-9bca0916a3-rboot.bin**. The upgrade package, on the other hand, includes the suffix '**-x86**', such as **picos-4.4.5-9bca0916a3-x86.bin**.

Partitioning

PICOS 4.0.0 have multiple system partitions including PicOS (partition size: 2G), PicOS2 (partition size: 2G) and User-Data partitions. Among them, PicOS and PicOS2 are two independent system boot partitions. One of them is the active partition on which the running system resides, and the other is the inactive partition. The two-system-boot-partition feature allows the system to be reverted to a previous version of the installed software package when it fails to upgrade PICOS.

User-Data partition is a reserved partition which is not affected by ONIE installer and upgrade unless user manually removes it. User-Data partition uses all the available space left on the disk after installation. Users can use this partition to store files and data.

Supported Platforms

PICOS 4.x software requires to run on a high performance device, only the platforms listed in Switch Machine Outline and System Characteristics are supported upgrading to PICOS 4.x.

Preparation before Upgrading

NOTE

If routed interface is configured, before upgrade, make sure that routed interface name and sub-interface name in the configuration file start with the string "**rif-**". Otherwise, upgrade will fail due to configuration error.

Table 1 Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build a different upgrade environment according to the need	
4	Getting the Required Upgrade Software	Obtain the required supported upgrade software	
5	Backing up Important Data in Flash	All the important data in Flash is backed up	
6	Checking Available Flash Space	Flash space is enough to save upgrading package and other files	

Checking the Running PicOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address : d4:31:27:c9:e4:51
Hardware Model : S5860-48MG-U
Linux System Version/Revision : 9.8.7-main/fd87d25a10
Linux System Released Date : 10/12/2024
L2/L3 Version/Revision : 9.8.7-main/fd87d25a10
L2/L3 Released Date : 10/12/2024
OVS/OF Version/Revision : 9.8.7-main/fd87d25a10
OVS/OF Released Date : 10/12/2024
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
{
  "Type":"1GE",
  "Feature":["Base Product", "Layer3", "OpenFlow"],
  "Support End Date":"2025-10-28",
  "Hardware ID":"ACD2-F77A-BBA3-2849",
  "Site Name":"PICA8"
```

```
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment, the basic requirements are as follows:

- PC can log in to the device through serial or SSH.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following website for the latest version of upgrade software.

https://www.pica8.com/support/

Backing up Important Data in Flash

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

Checking the Available Flash Space

Use the **df -h** command to check the available flash space for saving the upgrade package.

```
admin@PICOS:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 989M 0 989M 0% /dev
overlay 706M 57M 650M 8% /
tmpfs 1009M 0 1009M 0% /dev/shm
tmpfs 404M 5.9M 398M 2% /run
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 50M 192K 50M 1% /tmp
/dev/ubi1_0 863M 376M 483M 44% /mnt/open
```

Upgrading Notes

- Downgrade from PICOS version 4.x to 3.x or to a lower version is NOT supported by using **upgrade** command. You can use ONIE installation when you want to downgrade. For details about ONIE installation, please refer to Installing PICOS on Bare Metal Switches.
- License check is performed for upgrade:
  - If PICOS has a license installed before the upgrade, the license will be copied and activated after the upgrade. Please check this section for the PICOS Licenses.
  - If there is no license installed prior to upgrade, upgrade2 process can proceed but only the first four ports and the first two uplink ports (if exist) on the newly upgraded system can be used.
  - If the license has expired, it is not allowed to upgrade a major release (e.g. 4.1 to 4.2). However, it will not affect upgrading to a minor release (e.g. 4.1.1 to 4.1.2).
- You can log in to the switch through its console port or using SSH. After successful login, you can run commands on the command line interface (CLI) to upgrade the device.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image might be modified during download, and the upgrade will fail during the MD5 check.
- When upgrading, the installer checks whether there is a user-data partition. If there exists a User-Data partition, the installer only rewrites the running system boot partition (PicOS/ PicOS2) and installs the new installation package to this partition. However, if there is no User-Data partition, the installer removes all the partitions to rebuild a brand new NOS.

- All X86 platforms share one installation and upgrade package with the name fixed as: **onie-installer-picos-VERSION-x86.bin**, where **VERSION** is the release version. X86 platforms are listed below:
    - FS N9550-32D
    - FS N8550-64C
    - FS N5850-48S6Q
    - FS N8550-48B8C
    - FS N8550-32C
    - Edgecore AS4630-54PE
    - Edgecore AS5712-54X
    - Edgecore AS5812-54T
    - Edgecore AS5812-54X
    - Edgecore AS7312-54X
    - Edgecore AS7326-56X
    - Edgecore AS7712-32X
    - Edgecore AS7726-32X
    - Edgecore AS7816-64X
    - Edgecore AS5835-54X
    - Edgecore AS9716-32D
    - DELL N3248P-ON
    - DELL N3248PXE-ON
    - DELL N3224PX-ON
    - DELL N3248X-ON
    - DELL S4048-ON
    - DELL S4148F-ON
    - DELL S4148T-ON
    - DELL S4128F-ON
    - DELL S5224F-ON
    - DELL S5296F-ON
    - DELL S5212F-ON
    - DELL S5248F-ON
    - DELL Z9100-ON
    - DELL Z9264F-ON
    - DELL N3224T-ON
    - DELL S4128T-ON
- During the upgrade process, please ensure that the power supply is functioning normally; otherwise, power interruption during the upgrade process could cause unpredictable problems.
- In previous 4.x.x versions, PICOS allows the configuration of route leaking by importing BGP IPv4 routes from one user-defined VRF into another user-defined VRF, for example:
  set protocols bgp vrf vrf1 local-as 1
  set protocols bgp vrf vrf1 ipv4-unicast import vrf vrf2
  set protocols bgp vrf vrf2 local-as 2
  That will cause configuration from PICOS CLI is not consistent with FRR configuration. Specifically, FRR will add "set protocols bgp local-as 1" (local as number is same as the value in vrf1) to its configuration automatically, which is not in PICOS CLI. From version 4.4.0, if "set protocols bgp local-as 1" is not configured, the above configurations are not allowed.

Based on the above reasons, users are required to manually add the command "set protocols bgp local-as 1" (local as number is same as the value in vrf1) before the upgrade, if there's above configuration exists in the pre- upgrade version, thus to ensure that the configuration can be loaded successfully after the upgrade.

Usage of Upgrade Command

```
admin@PICOS:~$ sudo upgrade
USAGE
   Upgrade system with local new image
SYNOPSIS
   upgrade [image_name] [factory-default]
DESCRIPTION
   image_name - Image with bin format file(*.bin)
   factory-default - Recovery configuration to factory default
```

PICOS upgrade is done via the command "**upgrade**" in bash (launching a shell script named "upgrade.sh"). This script will upgrade the image and back up configuration files automatically.

The format of the upgrade package is ***.bin**.

The option **no-md5-check** is removed from PICOS 3.7.0 and later versions. If there is an MD5 file in the /cftmp directory, the upgrade script will check package integrity with MD5. Else if there is no MD5 file in the /cftmp directory, then skip the MD5 check step.

The option **factory-default** is used to reset the configuration to factory default when performing upgrade. This option retains the license files from the previous version.

If you want to backup a file during upgrade, use option **backup-file=(*.lst)** to define your own backup file list. The usage of option **backup-file=(*.lst)** is described in the below section.

Usage of Backup-file=(*.lst) Option

During the upgrade process, the switch can automatically back up the following files in the following directories from the previous PICOS system:

```
/etc/passwd
/etc/shadow
/etc/group
/etc/gshadow
/etc/resolv.conf
./etc/network/interfaces
/etc/picos/picos_start.conf
/etc/picos/switch-public.key
/etc/picos/pica.lic
/pica/config/pica_startup.boot
/pica/config/pica.conf.01
/pica/config/pica.conf.02
/pica/config/pica.conf.03
/pica/config/pica.conf.04
```

```
/pica/config/pica.conf.05
/ovs/ovs-vswitchd.conf.db
/ovs/function.conf.db
/ovs/config/meters
/ovs/config/groups
/ovs/config/flows
/ovs/var/lib/openvswitch/pki/
/var/log/report_diag.log
/var/log/report_diag.log.1
/var/log/report_diag.log.2
/var/log/report_diag.log.3
/var/log/report_diag.log.4
/var/log/report_diag.log.5
/cftmp/upgrade.log
/cftmp/upgrade2.log
/cftmp/auto/
```

If you want to save user files that are not in the above default backup file list, you need to first create or specify a **.lst** file and then add all those files that need to be backed up to this **.lst** file. You can use the **backup-file=(*.lst)** option to achieve this, where (*.lst) is the user created file with **.lst** format or specify the path to this file, for example:

```
admin@PICOS:~$ sudo upgrade backup-file=/admin/back_files.lst onie-installer-picos-4.0.1-x86.bin
```

For example, if you want to backup **/home/admin/a.txt** file during the process, then add **/home/admin/a.txt** to back_files.lst.In this example, **back_files.lst** is a user created file. The user has already added the file to back_files.lst that needs to be saved in the event of power off.

```
admin@PICOS:~$ cat /admin/back_files.lst
 /home/admin/a.txt
```

The above operations ensure that user can backup their important files with **backup-file=(*.lst)** option during the upgrade process.

Upgrading Procedure

The upgrading procedure in this document gives an example of upgrading AS7312-54X from PICOS 4.0.0 to 4.0.1.

Step1 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.16:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-4.0.1-x86.bin
/cftmp
admin@PICOS:~$ sudo scp pica8@10.10.50.16:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-4.0.1-x86.bin.md5
/cftmp
```

NOTE:

If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:

admin@Xorplus:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-91bb175.bin /cftmp

admin@Xorplus:~$sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-91bb175.bin.md5 /cftmp

If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the EVPN Multihoming Configuration Guide.

Step2 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step3 Change directory to /cftmp.

```
admin@PICOS:~$ cd /cftmp
admin@PICOS:/cftmp$
```

Step4 Run the **upgrade** command.

```
admin@PICOS:/cftmp$ sudo upgrade onie-installer-picos-4.0.1-x86.bin
```

After finishing upgrade will reboot automatically, the system will come up running the new network operating system.

Verifying Version after Upgrading

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address     : d4:31:27:c9:e4:51
Hardware Model                : as7312_54x
Linux System Version/Revision : 9.8.7-main/fd87d25a10
Linux System Released Date    : 10/12/2024
L2/L3 Version/Revision        : 9.8.7-main/fd87d25a10
L2/L3 Released Date           : 10/12/2024
OVS/OF Version/Revision       : 9.8.7-main/fd87d25a10
OVS/OF Released Date          : 10/12/2024
```

Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X

Installation or upgrade failure (for example, the switches cannot boot up after install) may occur on the old AS7326-56X hardware models (revision is R01F and before). When booting PICOS on AS7326-56X and detect hardware rev R01F, the system will log a warning message to prompt the hardware revision R01F is a pre-production hardware reversion: "This hardware revision R01F is a pre-production hardware rev, PICOS has applied a work around to work with PICOS. Support will be provided on a best effort basis".

To work around the issue, first we need to check the “Label Revision”. If it is an old hardware model (revision is R01F or before), then, we can perform the following provided solution after installation/upgrade to solve the problem.

Check Label Revision

Under ONIE prompt, run “**onie_syseeprom**” to get the “*Label Revision*”.

```
ONIE:/ # onie-syseeprom
TlvInfo Header:
```

```
   Id String:    TlvInfo
   Version:      1
   Total Length: 166
TLV Name             Code Len Value
-------------------- ---- --- -----
Manufacture Date     0x25  19 04/27/2019 02:10:06
Label Revision       0x27   4 R01B
Platform Name        0x28  27 x86_64-accton_as7326_56x-r0
ONIE Version         0x29  13 2018.05.00.05
Manufacturer         0x2B   6 Accton
Diag Version         0x2E   7 0.0.1.0
Base MAC Address     0x24   6 80:A2:35:81:D5:F0
Serial Number        0x23  14 732656X1916012
Country Code         0x2C   2 TW
Part Number          0x22  13 FP4ZZ7656005A
Product Name         0x21  15 7326-56X-O-AC-F
MAC Addresses        0x2A   2 256
Vendor Name          0x2D   6 Accton
CRC-32               0xFE   4 0xC3D3F2DE
Checksum is valid.
ONIE:/ #
```

Solution

You can follow the steps below after installation/upgrade, to fix the problem of installation and upgrade failure on the old AS7326-56X hardware model (revision R01F or before).

Step1 Power cycle the switch.

Step2 From the GRUB menu, choose “**ONIE”** to enter ONIE GRUB menu:

```
 +----------------------------------------------------------------------------+
 | PicOS                                                                      |
 |*ONIE                                                                       |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 +----------------------------------------------------------------------------+
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

Step3 From ONIE GRUB menu, choose “**ONIE: Rescue”** to launch ONIE in Rescue mode.

```
                         GNU GRUB  version 2.02~beta2+e4a1fe391
 +----------------------------------------------------------------------------+
 | ONIE: Install OS                                                           |
 |*ONIE: Rescue                                                               |
 | ONIE: Uninstall OS                                                         |
 | ONIE: Update ONIE                                                          |
 | ONIE: Embed ONIE                                                           |
 | DIAG: Accton Diagnostic                                                    |
```

```
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 +----------------------------------------------------------------------------+
```

Step4 Press Enter to display the ONIE prompt.

Step5 Mount PicOS partition with label is “PicOS”.

```
ONIE:/ # blkid
/dev/sda7: LABEL="User-Data" UUID="be63cef8-4560-4c48-ab5a-8f7ced5a950b"
/dev/sda6: LABEL="PicOS2" UUID="f589e53f-4cd1-44ba-8384-f339f4e2b2ac"
/dev/sda5: LABEL="PicOS" UUID="8ca5f7ed-5a15-4a2a-944c-4d8872647bf5"
/dev/sda4: LABEL="PICOS-GRUB" UUID="782a1372-4b66-4783-b920-dab1df8ec6e4"
/dev/sda3: LABEL="ACCTON-DIAG" UUID="3e4117d0-1926-472a-9d9e-08883df83d40"
/dev/sda2: LABEL="ONIE-BOOT" UUID="1a90abd8-f065-4f7a-90a0-af122b8805fa"
ONIE:/ #
ONIE:/ # mount /dev/sda5 /mnt
```

Step6 Execute the following command to modify the I2C access address.

```
ONIE:/ # sed -I "s/0x57/0x56/" /mnt/etc/rc_hw.sh
ONIE:/ # sync
```

Step7 Unmount the PicOS partition.

```
ONIE:/ # unmount /dev/sda5
```

Step8 Reboot the switch.

```
ONIE:/ # reboot
```

Upgrading PICOS from Version 3.0 or Later Using Upgrade2

- Introduction
- Preparation before Upgrading
  - Checking the Running PICOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data
  - Converting Configuration to 4.x before Upgrade (when Upgrade from Version 3.x to 4.x)
- Upgrading Notes
- Usage of Upgrade2 Command
  - Usage of use-prev-config Option
  - Usage of Backup-file=(*.lst) Option
- Upgrade Procedure
- Rollback Procedure
- Verifying Version after Upgrade
- Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X
  - Check Label Revision
  - Solution

Introduction

NOTE：

- This document **only** applies to PICOS upgrade from version 3.0 or later version using command **upgrade2**. If you want to upgrade PICOS from the version before 3.0, use ONIE installation process described in Installing PICOS on Bare Metal Switches.
- You cannot do a standard upgrade from 3.x to 4.x. This is because 3.x config and 4.x config are not compatible, and PICOS 4.x will not be able to boot with 3.x config after the upgrade. In order to upgrade from 3.x to 4.x, you MUST convert the configuration to 4.x before upgrade, see section Converting Configuration to 4.x before Upgrade (when Upgrade from Version 3.x to 4.x) in this guide for details.
- This upgrading guide is not available for FS S5810 Series and S5860 Series switches.
- N8560-32C uses the ONIE method for upgrade described in this guide, while the installation uses Rboot method, please refer to Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches for details on the installation process.
- The installation package name for N8560-32C includes the suffix '**-rboot**', for example, **N8560_picos-4.4.5-9bca0916a3-rboot.bin**. The upgrade package, on the other hand, includes the suffix '**-x86**', such as **picos-4.4.5-9bca0916a3-x86.bin**.

PICOS 4.0.0 and later versions have multiple system partitions including PicOS (partition size: 2G), PicOS2(partition size: 2G) and User-Data partitions. Among them, PicOS and PicOS2 are two independent system boot partitions. One of them is the active partition on which the running system resides, and the other is the inactive partition. The two-system-boot-partition feature allows the system to revert to a previous version of the installed software package when it fails to upgrade PICOS by using upgrade2 command.

User-Data partition is a reserved partition which is not affected by ONIE installer and upgrade unless user manually removes it. User-Data partition uses all the available space left on the disk. Users can use this partition to store files and data.

When running upgrade2, the new version PICOS image will be installed and boot onto the inactive partition automatically. Afterwards, the inactive partition will switch to active partition automatically when the switch boots up normally after the upgrading is finished, while the other partition where the old version resides will become the inactive partition.

Upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system. This can reduce the network interruption risk due to the failure of system upgrade process and ensure the systems' continuous availability. You can refer to section Rollback Procedure in this page for details.

The system also supports the **upgrade** method for PICOS version upgrade, you can refer to the document Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command for details. We recommend using upgrade2 method to upgrade the NOS as it includes system backup and rollback features.

Preparation before Upgrading

Table 1. Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed.	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build an upgrade environment according to the need.	
4	Getting the Required Upgrade Software	Obtain the required supported upgrade software.	
5	Backing up Important Data	All the important data was backed up.	
6	Converting Configuration to 4.x before Upgrade (when Upgrade from Version 3.x to 4.x)	4.x configuration is generated from 3.x configuration file.	

Checking the Running PICOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address : 64:9d:99:d8:fd:07
Hardware Model            : S3410-48TS-P
PICOS Release/Commit      : 4.4.4-s3000/eaf8c6573d
PICOS Released Date       : 09/14/2024
admin@PICOS:~$
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
```

```
{
  "Type":"1GE",
  "Feature":["Base Product", "Layer3", "OpenFlow"],
  "Support End Date":"2025-10-28",
  "Hardware ID":"ACD2-F77A-BBA3-2849",
  "Site Name":"PICA8"
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment, the basic requirements are as follows:

- PC can log in to the device through serial or SSH.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following webpage for the latest version of upgrade software.

https://www.pica8.com/support/

Backing up Important Data

Before upgrading, save the important data, e.g. the configuration file, to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed if needed.

Converting Configuration to 4.x before Upgrade (when Upgrade from Version 3.x to 4.x)

NOTE:

When upgrade PICOS from version 3.x to 4.x:

- When executing the **upgrade2** command, no other option is supported except the option **image_name**.
- Backup the configuration file before upgrading.
- The OVS configuration for crossflow before the upgrade will be saved and restored automatically after the upgrade.

You cannot do a standard upgrade from 3.x to 4.x. This is because 3.x configuration and 4.x configuration are not compatible, and PICOS 4.x will not be able to boot with 3.x configuration after the upgrade.

In order to upgrade from 3.x to 4.x, follow the procedure below to prepare the 4.x configuration file before upgrade:

1. Create directory */pica/config-4.x/*.
2. Contact Pica8 support to convert the 3.x configuration to 4.x configuration in configuration file *pica_startup.boot.*
3. Copy the 4.x configuration file (converted from 3.x configuration file in step 2) into the directory */pica/config-4.x* just created. After upgrading from 3.x to 4.x and after rebooting, PICOS 4.x will look for the 4.x configuration in */pica/config-4.x.*

After completing these steps, the 4.x configuration file is ready and you can continue with the upgrade process.

If these steps are not performed before upgrade, the system will load the default configuration file of 4.x and the 3.x configuration will not be loaded after upgrade. However, if this happens unexpectly, you can also remedy by loading the 4. x configuration file after upgrade, follow the steps below:

1. Copy the 4.x configuration file *pica_startup.boot* (already converted from 3.x configuration file) into the directory */pica/config/.*
2. Run the **load override** command to load 4. x configuration.

```
admin@PICOS# load override /pica/config/pica_startup.boot
admin@PICOS# Loading config file...
```

```
3 Config file was loaded successfully.
```

Upgrading Notes

- This upgrade2 guide only applies to PICOS upgrade from version 4.0.0 or the later versions.
- When using upgrade2 to upgrade PICOS, you should make sure the “PicOS2” partition exists.
- When using upgrade2 to upgrade PICOS, you should make sure the partition type is **GPT**.
- When using upgrade2 to upgrade PICOS, you should make sure that ONIE is pre-loaded.
- License check is performed for upgrade:
  - If PICOS has a license installed before the upgrade, the license will be copied and activated after the upgrade. Please check this section for the PICOS Licenses.
  - If there is no license installed prior to upgrade, upgrade2 process can proceed but only the first four ports and the first two uplink ports (if exist) on the newly upgraded system can be used.
  - If the license has expired, it is not allowed to upgrade a major release (e.g. 4.1 to 4.2). However, it will not affect upgrading to a minor release (e.g. 4.1.1 to 4.1.2).
- You can log in to a device through its console port or using SSH. After successful login, you can run commands on the command line interface (CLI) to upgrade the device.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image might be modified during download, and the upgrade will fail during the MD5 check.
- The image is platform dependent, that is, the image should be consistent with the platform, otherwise the upgrade script will abort.
- An upgrage2.log file in **/cftmp** directory will be created which will contain all the logs related to the upgrade2 process.
- All X86 platforms share one installation and upgrade package with the name fixed as: **onie-installer-picos-VERSION-x86.bin**, where **VERSION** is the release version. X86 platform are listed below:
  - FS N9550-32D
  - FS N8550-64C
  - FS N5850-48S6Q
  - FS N8550-48B8C
  - FS N8550-32C
  - Edgecore AS4630-54PE
  - Edgecore AS5712-54X
  - Edgecore AS5812-54T
  - Edgecore AS5812-54X
  - Edgecore AS7312-54X
  - Edgecore AS7326-56X
  - Edgecore AS7712-32X
  - Edgecore AS7726-32X
  - Edgecore AS7816-64X
  - Edgecore AS5835-54X
  - Edgecore AS9716-32D
  - DELL N3248P-ON
  - DELL N3248PXE-ON
  - DELL N3224PX-ON
  - DELL N3248X-ON
  - DELL S4048-ON
  - DELL S4148F-ON

    - DELL S4148T-ON
    - DELL S4128F-ON
    - DELL S5224F-ON
    - DELL S5296F-ON
    - DELL S5212F-ON
    - DELL S5248F-ON
    - DELL Z9100-ON
    - DELL Z9264F-ON
    - DELL N3224T-ON
    - DELL S4128T-ON
- In previous 4.x.x versions, PICOS allows the configuration of route leaking by importing BGP IPv4 routes from one user-defined VRF into another user-defined VRF, for example:
  set protocols bgp vrf vrf1 local-as 1
  set protocols bgp vrf vrf1 ipv4-unicast import vrf vrf2
  set protocols bgp vrf vrf2 local-as 2
  That will cause configuration from PICOS CLI is not consistent with FRR configuration. Specifically, FRR will add "set protocols bgp local-as 1" (local as number is same as the value in vrf1) to its configuration automatically, which is not in PICOS CLI. From version 4.4.0, if "set protocols bgp local-as 1" is not configured, the above configurations are not allowed.

Based on the above reasons, users are required to manually add the command "set protocols bgp local-as 1" (local as number is same as the value in vrf1) before the upgrade, if there's above configuration exists in the pre- upgrade version, thus to ensure that the configuration can be loaded successfully after the upgrade.

Usage of Upgrade2 Command

```
admin@PICOS:~$ sudo upgrade2
USAGE
   Upgrade system with local new image
SYNOPSIS
   upgrade2 [image_name] [factory-default]
DESCRIPTION
   image_name - Image with bin format file(*.bin)
   factory-default - Recovery configuration to factory default
admin@PICOS:~$
```

For PICOS **go2cli** version, users can run the upgrade2 command under CLI operational mode or configuration mode:

```
admin@PICOS> upgrade2 image-file xx.bin
Possible completions:
  <[Enter]>                      Execute this command
  backup-file                    Specify a user defined backup list(*.lst)
  factory-default                Recovery configuration to factory default
  use-prev-config                Use previous configuration, and syslog trace

admin@PICOS# run upgrade2 image-file xx.bin
Possible completions:
  <[Enter]>                      Execute this command
  backup-file                    Specify a user defined backup list(*.lst)
  factory-default                Recovery configuration to factory default
```

```
13  use-prev-config                Use previous configuration, and syslog trace
```

PICOS upgrade is done via the command "**upgrade2**" in bash (launching a shell script named "upgrade2.sh"). This script will upgrade the image and backup configuration files automatically.

Image name is in the form of **.bin**, which should be copied to the **/cftmp** directory before running upgrade2 command.

The option **factory-default** is used to reset the configuration to factory default when performing upgrade, but it retains the license files from the previous version.

If you want to use the old configuration file in the new version, you can add the **use-prev-config** option when issuing upgrade2 command. The usage of option **use-prev-config** is described in the section Usage of Use-prev-config Option.

If you want to backup a file during upgrade, use **backup-file=(*.lst)** option to define your own backup file list. The usage of **backup-file=(*.lst)** option is described in the section Usage of Backup-file=(*.lst) Option.

Usage of use-prev-config Option

The main function of **use-prev-config** option is to decide whether to load the previous configuration file after a system reboot when performing upgrade2 or rollback to another version. If there is a command line in the old version configuration file that is not supported in the new system, with **use-prev-config** option that command will be skipped and continue loading the remaining configuration.

By default, upgrade2 or rollback is performed without **use-prev-config** option.

The following table describes the usage of **use-prev-config** option when performing upgrade2 or rollback.

	upgrade2 (From old version to new version)	**rollback** (From current version to old version)
with use-prev-config	1. Load the configuration file of old version after system reboot. 2. If there is a command line in the old version configuration file that is not supported in the new system, skip it and continue loading the remaining configuration.	1. Load the configuration file of current version after system reboot. 2. If there is a command line in the current configuration file that is not supported in the old system, skip it and continue loading the remaining configuration.
without use-prev-config	1. Load the configuration file of old version after reboot. 2. If there is a command in the old version configuration file that is not supported in the new system, load default configuration file.	Load the old version configuration file after rebooting.

Usage of Backup-file=(*.lst) Option

During the upgrade process, the switch can automatically back up the following files in the following directories from the previous PICOS system:

```
/etc/passwd

/etc/shadow

/etc/group
```

```
/etc/gshadow
/etc/resolv.conf
./etc/network/interfaces
/etc/picos/picos_start.conf
/etc/picos/switch-public.key
/etc/picos/pica.lic
/pica/config/pica_startup.boot
/pica/config/pica.conf.01
/pica/config/pica.conf.02
/pica/config/pica.conf.03
/pica/config/pica.conf.04
/pica/config/pica.conf.05
/ovs/ovs-vswitchd.conf.db
/ovs/function.conf.db
/ovs/config/meters
/ovs/config/groups
/ovs/config/flows
/ovs/var/lib/openvswitch/pki/
/var/log/report_diag.log
/var/log/report_diag.log.1
/var/log/report_diag.log.2
/var/log/report_diag.log.3
/var/log/report_diag.log.4
/var/log/report_diag.log.5
/cftmp/upgrade.log
/cftmp/upgrade2.log
/cftmp/auto/
```

If you want to save user files that are not in the above default backup file list, you need to first create or specify a **.lst** file and then add all those files that need to be backed up to this **.lst** file. You can use the **backup-file=(*.lst)** option to achieve this, where (*.lst) is the user created file with **.lst** format or specify the file path to this file, for example:

```
admin@PICOS:~$ sudo upgrade2 backup-file=/admin/back_files.lst onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin
```

For example, if you want to backup **/home/admin/a.txt** file during the process, then add **/home/admin/a.txt** to back_files.lst. In this example, **back_files.lst** is a user created file. The user has already added the file to back_files.lst that needs to be saved in the event of power off.

```
admin@PICOS:~$ sudo upgrade2 backup-file=/admin/back_files.lst onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin
```

The above operations ensure that user can backup their important files with backup-file=(*.lst) option during the upgrade process.

Upgrade Procedure

The upgrading procedure in this document gives an example of upgrading from PICOS 4.0.0 to 4.0.1 using **upgrade2** command on AS7312_54X switch.

Step1 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin /cftmp
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin.md5 /cftmp
```

NOTE:

- If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:

admin@Xorplus:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin /cftmp

admin@Xorplus:~$sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.0.1/as7312_54x/onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin.md5 /cftmp

If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF Configuration Guide.

- For PICOS **go2cli** version, users can run the scp command under CLI operational mode or configuration mode:

Φ Download a file:

file scp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>:<*port*> [**vrf** <mgmt-vrf | *vrf-name*>]

Φ Upload a file:

file scp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>:<*port*> [**vrf** <mgmt-vrf | *vrf-name*>]

Step2 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step3 Change directory to **/cftmp**.

```
admin@PICOS:~$ cd /cftmp
```

Step4 Run **upgrade2** command to begin upgrading.

```
admin@PICOS:~$ sudo upgrade2 onie-installer-picos-as7312_54x-4.0.1-cc8d268.bin
```

After finishing upgrade, the switch will reboot automatically, the system will come up running the new network operating system.

NOTE：

- For PICOS **go2cli** version, users can run the upgrade2 command under CLI operational mode or configuration mode.

- It will take 20 - 30 minutes to finish upgrading PICOS. During the upgrade process, please be patient and do not perform any operation until the upgrade is complete, otherwise, the upgrade may be interrupted.

Rollback Procedure

The upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system.

NOTE：
Usage of **nos-rollback** command:

admin@Xorplus:~$ sudo nos-rollback

USAGE

Rollback to the previous system after next reboot

SYNOPSIS

nos-rollback [use-prev-config]

DESCRIPTION

use-prev-config - Use previous config, and syslog trace

For details about the usage of use-prev-config, please refer to Usage of Use-prev-config Option.

The rollback procedure is as follows:

Step1 Run **nos-rollback** command for manually rollback.

```
admin@PICOS:~$ sudo nos-rollback
USAGE
    Rollback to the previous system after next reboot
SYNOPSIS
    nos-rollback
Checking prerequisites
       Attribute of current system                          [OK]

Will switch from PICOS-4.4.5GA to the other system!
Do you want to continue?[y/N]?y

Updating default boot option
       Modify default boot option                           [OK]
Rollback to the other system successful!
Please reboot to enter the other system!
admin@PICOS:~$
```

Step2 Reboot system manually to finish rollback.

```
admin@Xorplus:~$ sudo reboot
```

You need to manually run reboot command to reboot the system after you have issued "**nos-rollback**" command. After rebooting successfully, the system will come up running the previous version of network operating system.

Verifying Version after Upgrade

```
admin@PICOS:~$ version
```

```
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address     : d4:31:27:c9:e4:51
Hardware Model                : S5860-48MG-U
Linux System Version/Revision : 4.4.5GA/7f06432992
Linux System Released Date    : 10/14/2024
L2/L3 Version/Revision        : 4.4.5GA/7f06432992
L2/L3 Released Date           : 10/14/2024
OVS/OF Version/Revision       : 4.4.5GA/7f06432992
OVS/OF Released Date          : 10/14/2024
```

Appendix: Troubleshooting Installation/Upgrade Failure on AS7326-56X

Installation or upgrade failure (for example, the switches cannot boot up after install) may occur on the old AS7326-56X hardware models (revision is R01F and before). When booting PICOS on AS7326-56X and detect hardware rev R01F, the system will log a warning message to prompt the hardware revision R01F is a pre-production hardware reversion: "This hardware revision R01F is a pre-production hardware rev, PICOS has applied a work around to work with PICOS. Support will be provided on a best effort basis".

To work around the issue, first we need to check the “Label Revision”. If it is an old hardware model (revision is R01F or before), then, we can perform the following provided solution after installation/upgrade to solve the problem.

Check Label Revision

Under ONIE prompt, run “**onie_syseeprom**” to get the “*Label Revision*”.

```
ONIE:/ # onie-syseeprom
TlvInfo Header:
   Id String:    TlvInfo
   Version:      1
   Total Length: 166
TLV Name             Code Len Value
-------------------- ---- --- -----
Manufacture Date     0x25  19 04/27/2019 02:10:06
Label Revision       0x27   4 R01B
Platform Name        0x28  27 x86_64-accton_as7326_56x-r0
ONIE Version         0x29  13 2018.05.00.05
Manufacturer         0x2B   6 Accton
Diag Version         0x2E   7 0.0.1.0
Base MAC Address     0x24   6 80:A2:35:81:D5:F0
Serial Number        0x23  14 732656X1916012
Country Code         0x2C   2 TW
Part Number          0x22  13 FP4ZZ7656005A
Product Name         0x21  15 7326-56X-O-AC-F
MAC Addresses        0x2A   2 256
Vendor Name          0x2D   6 Accton
CRC-32               0xFE   4 0xC3D3F2DE
Checksum is valid.
ONIE:/ #
```

Solution

You can follow the steps below after installation/upgrade, to fix the problem of installation and upgrade failure on the old AS7326-56X hardware model (revision R01F or before).

Step1 Power cycle the switch.

Step2 From the GRUB menu, choose “**ONIE”** to enter ONIE GRUB menu:

```
+----------------------------------------------------------------------------+
| PicOS                                                                      |
|*ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Step3 From ONIE GRUB menu, choose “**ONIE: Rescue”** to launch ONIE in Rescue mode.

```
                         GNU GRUB  version 2.02~beta2+e4a1fe391
+----------------------------------------------------------------------------+
| ONIE: Install OS                                                           |
|*ONIE: Rescue                                                               |
| ONIE: Uninstall OS                                                         |
| ONIE: Update ONIE                                                          |
| ONIE: Embed ONIE                                                           |
| DIAG: Accton Diagnostic                                                    |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
```

Step4 Press Enter to display the ONIE prompt.

Step5 Mount PicOS partition with label is “PicOS”.

```
ONIE:/ # blkid
/dev/sda7: LABEL="User-Data" UUID="be63cef8-4560-4c48-ab5a-8f7ced5a950b"
/dev/sda6: LABEL="PicOS2" UUID="f589e53f-4cd1-44ba-8384-f339f4e2b2ac"
/dev/sda5: LABEL="PicOS" UUID="8ca5f7ed-5a15-4a2a-944c-4d8872647bf5"
/dev/sda4: LABEL="PICOS-GRUB" UUID="782a1372-4b66-4783-b920-dab1df8ec6e4"
/dev/sda3: LABEL="ACCTON-DIAG" UUID="3e4117d0-1926-472a-9d9e-08883df83d40"
/dev/sda2: LABEL="ONIE-BOOT" UUID="1a90abd8-f065-4f7a-90a0-af122b8805fa"
ONIE:/ #
ONIE:/ # mount /dev/sda5 /mnt
```

Step6 Execute the following command to modify the I2C access address.

```
ONIE:/ # sed -I "s/0x57/0x56/" /mnt/etc/rc_hw.sh
ONIE:/ # sync
```

Step7 Unmount the PicOS partition.

```
ONIE:/ # unmount /dev/sda5
```

Step8 Reboot the switch.

```
ONIE:/ # reboot
```

Installing Debian Packages on PICOS

PICOS uses a standard and non-modified Debian Linux distribution. It is very easy to install new packages or software on top of the existing PICOS packages, using the standard Debian package management system.

Here are some installation examples.

Installing GCC on PicOS

Installing Puppet on PicOS

Installing Salt on PicOS

Installing GCC on PicOS

NOTE:
If the FTP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the apt-get command when executing the apt-get operation.

For example:

admin@Xorplus:~$ sudo ip vrf exec mgmt-vrf apt-get update

If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF configuration guide.

Updating the software list on the source server

```
admin@XorPlus$sudo apt-get update
Hit http://ftp.tw.debian.org stable Release.gpg
Hit http://ftp.tw.debian.org stable Release
Hit http://ftp.tw.debian.org stable/main powerpc Packages
Hit http://ftp.tw.debian.org stable/main Translation-en
Reading package lists... Done
admin@XorPlus$
```

Installing new software

```
admin@XorPlus$sudo apt-get install make
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
make-doc
The following NEW packages will be installed:
make
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 399 kB of archives.
After this operation, 1165 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
make
Authentication warning overridden.
Get:1 http://ftp.tw.debian.org/debian/ stable/main make powerpc 3.81-8.2 [399 kB]
Fetched 399 kB in 6s (64.1 kB/s)
Selecting previously unselected package make.
(Reading database ... 16155 files and directories currently installed.)
Unpacking make (from .../make_3.81-8.2_powerpc.deb) ...
Processing triggers for man-db ...
fopen: Permission denied
Setting up make (3.81-8.2) ...
admin@XorPlus$
admin@XorPlus$sudo apt-get install python
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
file libexpat1 libmagic1 mime-support python-minimal python2.7 python2.7-minimal
Suggested packages:
python-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
file libexpat1 libmagic1 mime-support python python-minimal python2.7 python2.7-minimal
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 5045 kB of archives.
After this operation, 18.3 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
WARNING: The following packages cannot be authenticated!
libmagic1 libexpat1 file mime-support python2.7-minimal python2.7 python-minimal python
Authentication warning overridden.
Get:1 http://ftp.tw.debian.org/debian/ stable/main libmagic1 powerpc 5.11-2 [201 kB]
```

```
Get:2 http://ftp.tw.debian.org/debian/ stable/main libexpat1 powerpc 2.1.0-1 [142 kB]
Get:3 http://ftp.tw.debian.org/debian/ stable/main file powerpc 5.11-2 [51.7 kB]
Get:4 http://ftp.tw.debian.org/debian/ stable/main mime-support all 3.52-1 [35.5 kB]
Get:5 http://ftp.tw.debian.org/debian/ stable/main python2.7-minimal powerpc 2.7.3-6 [1753 kB]
Get:6 http://ftp.tw.debian.org/debian/ stable/main python2.7 powerpc 2.7.3-6 [2639 kB]
Get:7 http://ftp.tw.debian.org/debian/ stable/main python-minimal all 2.7.3-4 [42.6 kB]
Get:8 http://ftp.tw.debian.org/debian/ stable/main python all 2.7.3-4 [180 kB]
Fetched 5045 kB in 18s (267 kB/s)
Selecting previously unselected package libmagic1:powerpc.
(Reading database ... 16189 files and directories currently installed.)
Unpacking libmagic1:powerpc (from .../libmagic1_5.11-2_powerpc.deb) ...
Selecting previously unselected package libexpat1:powerpc.
Unpacking libexpat1:powerpc (from .../libexpat1_2.1.0-1_powerpc.deb) ...
Selecting previously unselected package file.
Unpacking file (from .../file_5.11-2_powerpc.deb) ...
Selecting previously unselected package mime-support.
Unpacking mime-support (from .../mime-support_3.52-1_all.deb) ...
Selecting previously unselected package python2.7-minimal.
Unpacking python2.7-minimal (from .../python2.7-minimal_2.7.3-6_powerpc.deb) ...
Selecting previously unselected package python2.7.
Unpacking python2.7 (from .../python2.7_2.7.3-6_powerpc.deb) ...
Selecting previously unselected package python-minimal.
Unpacking python-minimal (from .../python-minimal_2.7.3-4_all.deb) ...
Selecting previously unselected package python.
Unpacking python (from .../python_2.7.3-4_all.deb) ...
Processing triggers for man-db ...
fopen: Permission denied
Setting up libmagic1:powerpc (5.11-2) ...
Setting up libexpat1:powerpc (2.1.0-1) ...
Setting up file (5.11-2) ...
Setting up mime-support (3.52-1) ...
Setting up python2.7-minimal (2.7.3-6) ...
Linking and byte-compiling packages for runtime python2.7...
Setting up python2.7 (2.7.3-6) ...
Setting up python-minimal (2.7.3-4) ...
Setting up python (2.7.3-4) ...
admin@XorPlus$
admin@XorPlus$sudo apt-get install g++
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
g+-4.6 libstdc+6-4.6-dev
Suggested packages:
g+-multilib g-4.6-multilib gcc-4.6-doc libstdc6-4.6-dbg libstdc+6-4.6-doc
The following NEW packages will be installed:
g++ g+-4.6 libstdc+6-4.6-dev
0 upgraded, 3 newly installed, 0 to remove and 17 not upgraded.
Need to get 0 B/8383 kB of archives.
After this operation, 24.4 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
WARNING: The following packages cannot be authenticated!
libstdc+6-4.6-dev g-4.6 g+
Authentication warning overridden.
Selecting previously unselected package libstdc++6-4.6-dev.
(Reading database ... 19555 files and directories currently installed.)
Unpacking libstdc+6-4.6-dev (from .../libstdc+6-4.6-dev_4.6.3-14_powerpc.deb) ...
Selecting previously unselected package g++-4.6.
Unpacking g+-4.6 (from .../g+-4.6_4.6.3-14_powerpc.deb) ...
Selecting previously unselected package g++.
Unpacking g++ (from .../g++_4%3a4.6.3-8_powerpc.deb) ...
Processing triggers for man-db ...
Setting up libstdc++6-4.6-dev (4.6.3-14) ...
Setting up g++-4.6 (4.6.3-14) ...
Setting up g++ (4:4.6.3-8) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
admin@XorPlus$
```

Installing Puppet on PicOS

NOTE:

- You can see an example of Puppet module to manipulate PicOS configuration on our Github repository:

  https://github.com/Pica8/Configuration-Managers

- If the FTP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the apt-get command when executing the apt-get operation.

  For example:

  admin@Xorplus:~$ sudo ip vrf exec mgmt-vrf apt-get update

  If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF configuration guide.

Step 1 Use the correct repository for the specific application and CPU on the switch. Pica8 support can help in the choice of repository.

```
admin@PICOS:~$sudo more /etc/apt/sources.list | grep -v "#"
deb http://ftp.debian-ports.org/debian/ unstable main
```

For a typical puppet installation, the latest standard debian repo is advised.

Step 2 Update the debian packages on PicOS.

```
admin@PICOS:~$ sudo apt-get update
Hit http://ftp.tw.debian.org stable Release.gpg
Hit http://ftp.tw.debian.org stable Release
Hit http://ftp.tw.debian.org stable/main powerpc Packages
Hit http://ftp.tw.debian.org stable/main Translation-en
Reading package lists... Done
admin@PICOS:~$
```

Step 3 Install puppet client and configure it.

```
admin@PICOS:~$ sudo apt-get install puppet
```

Look at the puppet documentation to understand how to connect the puppet client to a puppet server. A simple installation would require at least minor modification on the puppet.conf file.

```
more /etc/puppet/puppet.conf
[agent]
server = master.local.pica8.com
```

Step 4 Verify Puppet installation.

```
admin@PICOS:~$ sudo puppet agent -t
Notice: Using less secure serialization of reports and query parameters for compatibility
Notice: with older puppet master. To remove this notice, please upgrade your master(s)
```

```
Notice: to Puppet 3.3 or newer.
Notice: See http://links.puppetlabs.com/deprecate_yaml_on_network for more information.
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts in /var/lib/puppet/lib/facter/facter_dot_d.rb
Info: Loading facts in /var/lib/puppet/lib/facter/root_home.rb
Info: Loading facts in /var/lib/puppet/lib/facter/puppet_vardir.rb
Info: Loading facts in /var/lib/puppet/lib/facter/pe_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/instance_id.rb
Info: Caching catalog for Roma
Info: Applying configuration version '1405148228'
Notice: Finished catalog run in 0.35 seconds
```

Installing Salt on PicOS

NOTE:

- You can see an example of Salt module to manipulate PicOS configuration on our Github repository:

  https://github.com/pica8/Configuration-Managers

- If the FTP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the apt-get command when executing the apt-get operation.

  For example:

  admin@Xorplus:~$ sudo ip vrf exec mgmt-vrf apt-get update

- If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF configuration guide.

Step 1 Use the correct repository for the specific application and CPU on the switch. Pica8 support can help in the choice of repository.

```
admin@PICOS:~$ sudo more /etc/apt/sources.list | grep -v "#"
deb http://ftp.debian-ports.org/debian/ unstable main
```

For a typical salt installation, the latest standard debian repo is advised.

Step 2 - Update the debian packages on PicOS

```
admin@PICOS:~$ sudo apt-get update
Hit http://ftp.tw.debian.org stable Release.gpg
Hit http://ftp.tw.debian.org stable Release
Hit http://ftp.tw.debian.org stable/main powerpc Packages
Hit http://ftp.tw.debian.org stable/main Translation-en
Reading package lists... Done
admin@PICOS:~$
```

Step 3 - Install salt-common and salt-minion and configure it

```
admin@PICOS:~$ sudo apt-get install salt-common
admin@PICOS:~$ sudo apt-get install salt-minion
```

Look at the salt documentation to understand how to connect the salt-minion to a salt-master. A simple installation would need at least minor modification on the minion configuration file.

```
more /etc/salt/minion
# Set the location of the salt master server, if the master server cannot be
# resolved, then the minion will fail to start.
master: salt.example.com
```

PICOS Installation and Upgrade Guide for FS S5810 Series, S3410 Series, S5860 Series and N8560-32C Switches

- Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Console Port)
- Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Console Port)
- Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches
- Installing PICOS for FS S3410 Series Switches
- Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Eth0 or Inband Management Interface)
- Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Eth0 or Inband Management Interface)

Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Console Port)

- Preparation before Upgrading
  - Checking the Running PICOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data in Flash
  - Checking Available Flash Space
  - Upgrading Notes
- Upgrading Procedure
- Verifying Version after Upgrading

> **NOTE:**
> This guide is only available for upgrading PICOS for FS S5810/S5860 Series switches when login via the **console port**.

Preparation before Upgrading

Table 1 Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build a different upgrade environment to get the upgrade software according to the need	
4	Getting the Required Upgrade Software	Obtain the required supporting upgrade software	
5	Backing up Important Data in Flash	All the important data in Flash is backed up	
6	Checking Available Flash Space	Flash space is enough to save upgrading package and other files	

Checking the Running PICOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS:~$ version
Copyright (C) 2009-2023 Pica8, Inc.
==================================
Base ethernet MAC Address     : 64:9d:99:d7:7d:23
Hardware Model                : S5810-48TS-P
Linux System Version/Revision : 4.3.3.1/4f6f523
Linux System Released Date    : 12/10/2023
L2/L3 Version/Revision        : 4.3.3.1/4f6f523
L2/L3 Released Date           : 12/10/2023
OVS/OF Version/Revision       : 4.3.3.1/4f6f523
OVS/OF Released Date          : 12/10/2023
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
{
"Type":"1GE",
"Feature":["Base Product", "Layer3", "OpenFlow"],
"Support End Date":"2020-10-28",
```

```
"Hardware ID":"ACD2-F77A-BBA3-2849",
"Site Name":"PICA8"
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment to get the upgrade software, the basic requirements are as follows:

- PC can log in to the device through serial.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following website for the latest version of upgrade software.

http://www.pica8.com/support/customer

Backing up Important Data in Flash

Before upgrading, save the important data (such as the configuration file) in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

> Where is the PicOS configuration?
>
> OVSDB file
>
> L2/L3 Configuration Files

Checking Available Flash Space

Use the **df** command to check the available flash space.

```
admin@PICOS:~$ df
Filesystem     1K-blocks   Used Available Use% Mounted on
udev              493028      0    493028   0% /dev
overlay           358904  57528    301376  17% /
tmpfs             512720      0    512720   0% /dev/shm
tmpfs             205088   3256    201832   2% /run
tmpfs               5120      0      5120   0% /run/lock
tmpfs              51200    292     50908   1% /tmp
/dev/ubi1_0       402660 208320    189500  53% /mnt/open
```

Upgrading Notes

- The device is not supported to upgrade to a previous version.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image can be modified during download, and the upgrade will fail during the md5 check.
- The image is platform dependent, that is, the image_name should be consistent with the platform, otherwise the upgrade script will abort.
- The image file is a **.bin** file, for example S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin.
- When upgrading, the installer checks whether there is a user-data partition. If there exists a User-Data partition, the installer only rewrites the running system boot partition (PicOS/PicOS2) and installs the new installation package to this partition. However, if there is no User-Data partition, the installer removes all the partitions to rebuild a brand new NOS.
- Upgrade operation via upgrade commands is not allowed on non-default system, you can upgrade PICOS only on default system. When there are more than one PICOS, the default system is the one automatically booted into after system reboot.
- During the upgrade process, no power interruption is allowed.

Upgrading Procedure

NOTE :

Usage of **upgrade** command:

admin@PICOS:~$ sudo upgrade

USAGE

Upgrade system with local new image

SYNOPSIS

upgrade [image_name] [factory-default]

DESCRIPTION

image_name - Image with bin format file(*.bin)

factory-default - Recovery configuration to factory default

- PICOS upgrade is done via the command "**upgrade**" in bash (launching a shell script named "upgrade.sh"). This script will upgrade the image automatically.
- The file format of the upgrade package is ***.bin**.
- If there is an MD5 file in the /cftmp directory, the upgrade script will check package integrity with MD5. Else if there is no MD5 file in the /cftmp directory, then skip the MD5 check step.
- The option **factory-default** is used to reset the configuration to factory default when performing upgrade. This option retains the license files from the previous version.

The upgrading procedure in this document gives an example of upgrading on S5810-48TS-P from PICOS 4.4.3.1 to 4.4.3.2.

Step1 Stop PICOS service before upgrade. On FS S5810 Series and S5860 Series switches, use the following command:

```
admin@PICOS:~$ sudo systemctl stop picos
```

Step2 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5810/S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin  /cf
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5810/S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin.md5
```

NOTE:
If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:

admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5810/S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin /cftmp

admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5810/S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin.md5 /cftmp

If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF Configuration Guide.

Step3 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step4 Change directory to /cftmp.

```
admin@PICOS:~$ cd /cftmp
```

Step5 Run the **upgrade** command.

```
admin@PICOS:~$ sudo upgrade S5810-48TS-P-picos-e-4.4.3.2-2f6f578-fs.bin
```

After the upgrade is complete, the system will automatically reboot and run the new network operating system.

Verifying Version after Upgrading

```
admin@PICOS:~$ version
Copyright (C) 2009-2023 Pica8, Inc.
==================================
Base ethernet MAC Address     : 64:9d:99:d7:7d:23
Hardware Model                : S5810-48TS-P
Linux System Version/Revision : 4.4.3.2/2f6f578
Linux System Released Date    : 12/15/2023
L2/L3 Version/Revision        : 4.4.3.2/2f6f578
L2/L3 Released Date           : 12/15/2023
OVS/OF Version/Revision       : 4.4.3.2/2f6f578
OVS/OF Released Date          : 12/15/2023
```

Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Console Port)

- Introduction
- Preparation before Upgrading
  - Checking the Running PICOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data in Flash
- Upgrading Notes
- Upgrading Procedure
  - NOTE:
- Rollback Procedure
- Verifying Version after Upgrading

NOTE:

- This guide is only available for upgrading PICOS for FS S5860 Series and S3410 Series switches when login via the **console port**.
- The S3410 Series switches only support upgrade via the upgrade2 method.
- S5810 Series switches only support the **upgrade** method and do not support the **upgrade2** method.

Introduction

PICOS supports **upgrade2** method for system upgrade. There will be two separate systems on the device after the upgrade2 operation: PICOS and PICOS2. One of them will be the running system and the other will stay inactive. PICOS and PICOS2 system files and their respective configuration files are located in ***/mnt/open/picos/*** of the flash. A list and brief description of these files is as follows.

```
* uImage1.itb
* picos1.sqsh
* config1/backup_files              //User-defined backup files list
* config1/backup.tar.gz                  //Backup of latest.tar.gz
* config1/latest.tar.gz              //The newest configuration files
* uImage2.itb
* picos2.sqsh
* config2/backup_files
* config2/backup.tar.gz
* config2/latest.tar.gz
```

The upgrade2 installer installs the new system into the inactive system's file. The inactive system will be overwritten. After this operation, the new system is the inactive system and then the installer modifies the boot menu to make the newly installed system to be the default boot system. Finally, the system will come up running the new network operating system when boots up normally after the upgrading is finished,.

Upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system. This can reduce the network interruption risk due to the failure of system upgrade process and ensure the systems' continuous availability. You can refer to section Rollback Procedure for details.

We recommend using upgrade2 method to upgrade the NOS as there are functions of system backup and rollback.

Preparation before Upgrading

Table 1. Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed.	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond	

		the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build an upgrade environment to get the upgrade software according to the need.	
4	Getting the Required Upgrade Software	Obtain the required supporting upgrade software.	
5	Backing up Important Data in Flash	All the important data in Flash is backed up.	

Checking the Running PICOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS# run show version
Copyright (C) 2009-2023 Pica8, Inc.
==================================
Base ethernet MAC Address     : 64:9d:99:d2:04:53
Hardware Model                : S5860-24XB-U
Linux System Version/Revision : 4.3.3.2/4b5f523
Linux System Released Date    : 12/14/2023
L2/L3 Version/Revision        : 4.3.3.2/4b5f523
L2/L3 Released Date           : 12/14/2023
OVS/OF Version/Revision       : 4.3.3.2/4b5f523
OVS/OF Released Date          : 12/14/2023
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
{
"Type":"1GE",
"Feature":["Base Product", "Layer3", "OpenFlow"],
"Support End Date":"2020-10-28",
"Hardware ID":"ACD2-F77A-BBA3-2849",
"Site Name":"PICA8"
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment to get the upgrade software, the basic requirements are as follows:

- PC can log in to the device through serial.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following website for the latest version of upgrade software.

http://www.pica8.com/support/customer

Backing up Important Data in Flash

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

Upgrading Notes

- Downgrade to an earlier version is NOT supported by using upgrade2 command.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image can be modified during download, and the upgrade will fail during the md5 check.
- The image file is a **.bin** file, for example S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin.
- The image is platform dependent, that is, the image_name should be consistent with the platform, otherwise the upgrade script will abort.

Upgrading Procedure

The upgrading procedure in this document gives an example of upgrading on S5860-24XB-U from PICOS 3.1.0 to 3.1.1 using **upgrade2** command.

> **NOTE：**
>
> Usage of **upgrade2** command:
>
> USAGE
>
> Upgrade system with local new image
>
> SYNOPSIS
>
> upgrade2 [image_name] [factory-default]
>
> DESCRIPTION
>
> image_name - Image with bin format file(*.bin)
> factory-default - Recovery configuration to factory default
>
> PICOS upgrade is done via the command "**upgrade2**" in bash (launching a shell script named "upgrade2.sh"). This script will upgrade the image and back up configuration files automatically.

> Image name is in the form of **.bin** from version 3.1.0, which should be copied to the /cftmp directo before running upgrade2 command.
>
> The **no-md5-check** option is removed from PICOS 3.1.0. If there is an MD5 file in the /cftmp directory, the upgrade script will check package integrity with MD5. Else if there is no MD5 file in the /cftmp directory, then skip the MD5 check step.
>
> The option **factory-default** is used to reset the configuration to factory default when performing upgrade, but it retains the license files from the previous version.

Upgrade2 Procedure

Step1 Stop PICOS service before upgrade.

- On FS S5810 Series and S5860 Series switches, use the following command:

```
admin@PICOS:~$ sudo systemctl stop picos
```

- On S3410 Series switches, use the following command:

```
admin@PICOS:~$ sudo /etc/init.d/picos stop
```

Step2 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/S5860-24XB-U/S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin  /cft
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/S5860-24XB-U/S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin.md5
```

> **NOTE:**
>
> If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:
>
> admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.4.3.2/S5860-24XB-U/S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin /cftmp
>
> admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/4.4.3.2/S5860-24XB-U/S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin.md5 /cftmp
>
> If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF Configuration Guide.

Step3 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step4 Change directory to **/cftmp**.

```
admin@PICOS:~$ cd /cftmp
```

Step5 Run **upgrade2** command to begin upgrading.

```
admin@PICOS:~$ sudo upgrade2 S5860-24XB-U-picos-e-4.4.3.2-2f6f578-fs.bin
```

After finishing upgrade, the switch will reboot automatically, the system will come up running the new network operating system.

> **NOTE：**
>
> It will take 20 - 30 minutes to finish upgrading PICOS. During the upgrade process, please be patient and do not perform any operation until the upgrade is complete, otherwise, the upgrade may be interrupted.

Rollback Procedure

The upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system.

> **NOTE：**
>
> Usage of **nos-rollback** command:
>
> admin@PICOS:~$ sudo nos-rollback
>
> USAGE
>
> Rollback to the previous system after next reboot
>
> SYNOPSIS
>
> nos-rollback

The rollback procedure is as follows:

Step1 Run **nos-rollback** command for manually rollback.

```
admin@PICOS:~$ sudo nos-rollback
```

Step2 Reboot system manually to finish rollback.

```
admin@PICOS:~$ sudo reboot
```

You need to manually reboot the system after issued "**nos-rollback**" command and the system switching takes effect. After rebooting successfully, the system will come up running the previous version of network operating system.

Verifying Version after Upgrading

```
admin@PICOS# run show version
Copyright (C) 2009-2023 Pica8, Inc.
================================
Base ethernet MAC Address     : 64:9d:99:d2:04:53
Hardware Model                : S5860-24XB-U
Linux System Version/Revision : 4.3.3.3/4c5a643
Linux System Released Date    : 12/26/2023
L2/L3 Version/Revision        : 4.3.3.3/4c5a643
L2/L3 Released Date           : 12/26/2023
OVS/OF Version/Revision       : 4.3.3.3/4c5a643
```

```
11 OVS/OF Released Date          : 12/26/2023
```

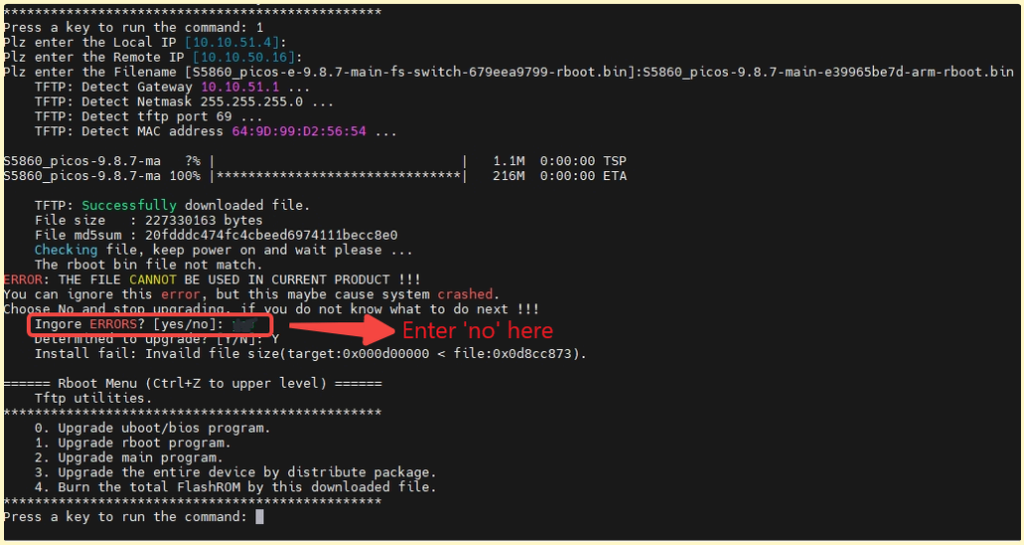
Installing PICOS for FS S5810/S5860 Series and N8560-32C Switches

NOTE:

- N8560-32C uses the Rboot method for installation described in this guide, while upgrade still uses the ONIE method, please refer to Upgrading PICOS from Version 3.0 or Later Using Upgrade2 and Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command for details on the upgrade process.
- The installation package name for N8560-32C includes the suffix '**-rboot**', for example, **N8560_picos-4.4.5-9bca0916a3-rboot.bin**. The upgrade package, on the other hand, includes the suffix '**-x86**', such as **picos-4.4.5-9bca0916a3-x86.bin**.

Caution:

When an incorrect installation file is detected, the system will display the error message "**Ignore ERRORS? [YES/NO]:**". Users need to enter "**no**" to prevent the system from using the incorrect installation file for system installation. Do NOT enter "yes", or the system will proceed with the incorrect installation file, which may cause a system crash.



PICOS system can be installed under the Rboot menu through TFTP protocol for FS S5810 and S5860 Series switches. The following steps describe the installation procedure.

Step 1 Power off and on to force restarting the switch, then press **Ctrl+C** to enter Rboot menu.

Step 2 (Optional) If the TFTP server and the switch are in the different network segment, configure the gateway address first (if they are in the same network segment, no need to do this step).

a) Enter **4** in the Rboot menu to access the *Scattered utilities* menu.

```
I2C:   ready
DRAM:  1 GiB
NAND:  1024 MiB
Loading Environment from SPI Flash... SF: Detected s25fl128s_64k
OK
Boot:   Master
Press Ctrl+B to enter Boot Menu, Press Ctrl+C to enter Rboot  0
[    1.529041] TIPC: Activated (version 2.0.0)
[    1.534192] TIPC: Started in single node mode

Rboot                          Version: 1.1.61
-------------------------------------------

    Mount rootfs1 ...
    Mount fail: Unknown storage type.
starting pid 964, tty '/dev/console': '-/etc/main_redirect'
starting pid 1084, tty '/dev/console': '-/etc/menu/menu_init'
====== Rboot Menu (Ctrl+Z to upper level) ======
    TOP menu items.
***********************************************
    0. Tftp utilities.
    1. X/Y/ZModem utilities.
    2. Run main.
    3. SetMac utilities.
    4. Scattered utilities.
***********************************************
Press a key to run the command: 4
====== Rboot Menu (Ctrl+Z to upper level) ======
    Scattered utilities.
***********************************************
    0. Show Version.
    1. Reload System.
    2. Set Baudrate.
    3. Format Flash.
    4. Exit menu.
    5. Set debug mode.
    6. Run main without enable password.
    7. Set Download Gateway.
***********************************************
Press a key to run the command: 7
Plz enter the Local GatewayIP [<NULL>]:10.10.51.1
Plz enter the IP Netmask [<NULL>]:255.255.255.0
    Set Local GatewayIP to 10.10.51.1
    Set IP Netmask to 255.255.255.0
```

b) Enter **7** to set the gateway IP and IP netmask.

c) Then, press **Ctrl+Z** to go back to the Rboot menu.

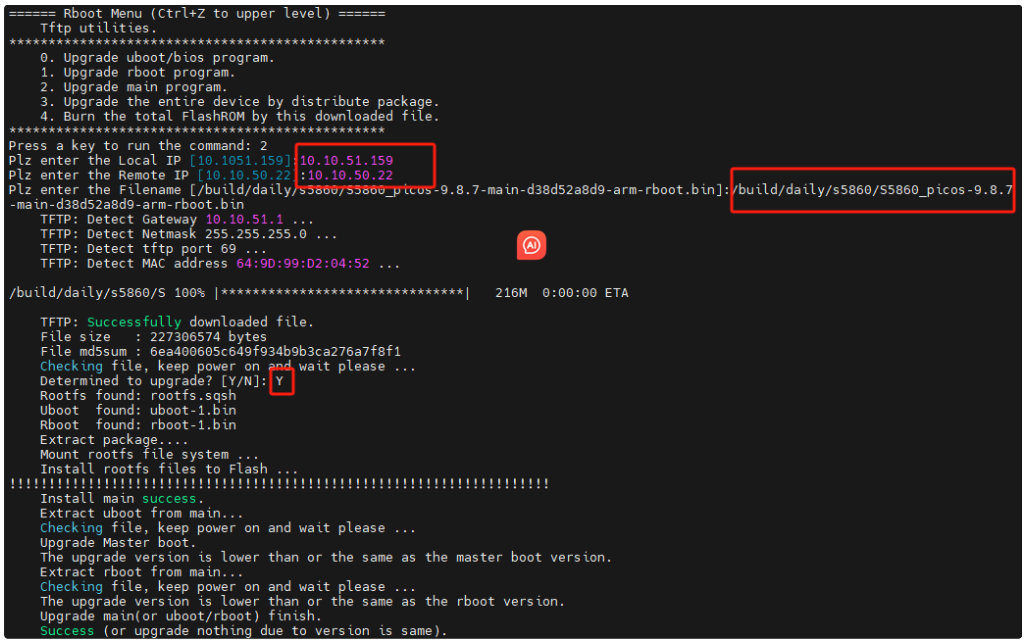
Step 3 In Rboot menu, enter **0** to access *Tftp utilities* menu, and then enter **2** to perform TFTP upgrade.

```
====== Rboot Menu (Ctrl+Z to upper level) ======
    TOP menu items.
***********************************************
    0. Tftp utilities.
    1. X/Y/ZModem utilities.
    2. Run main.
    3. SetMac utilities.
    4. Scattered utilities.
***********************************************
Press a key to run the command: 0
====== Rboot Menu (Ctrl+Z to upper level) ======
    Tftp utilities.
***********************************************
    0. Upgrade uboot/bios program.
    1. Upgrade rboot program.
    2. Upgrade main program.
    3. Upgrade the entire device by distribute package.
    4. Burn the total FlashROM by this downloaded file.
***********************************************
Press a key to run the command: 2
```

Step 4 Use TFTP protocol to download the installation files, and then install PICOS.

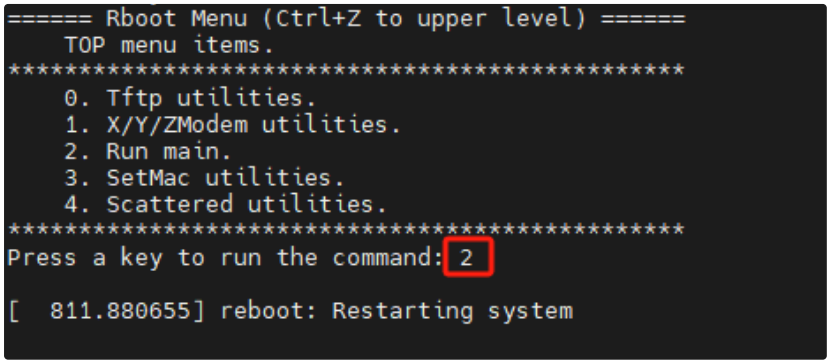
a) Configure the TFTP parameters. **Local IP** is the management interface IP of the switch, **Remote IP** is the IP of the TFTP server, **Filename** is the installation image directory and name located on the TFTP server.

b) After downloaded the installation image successfully, you need to input **Y** manually, then the system will automatically start system installation process.



Wait a few minutes before the installation process is completed. When **Success** is displayed, it indicates that the installation process is successfully completed.

Step 5 Press **Ctrl+Z** to go back to the Rboot menu, then type **2** to reboot the switch.



Then the device reboots and comes up running the new network operating system.

Users need to enter the username and password after the system restarts, the initial login username is admin and password is pica8. Then users will be asked to set a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Installing PICOS for FS S3410 Series Switches

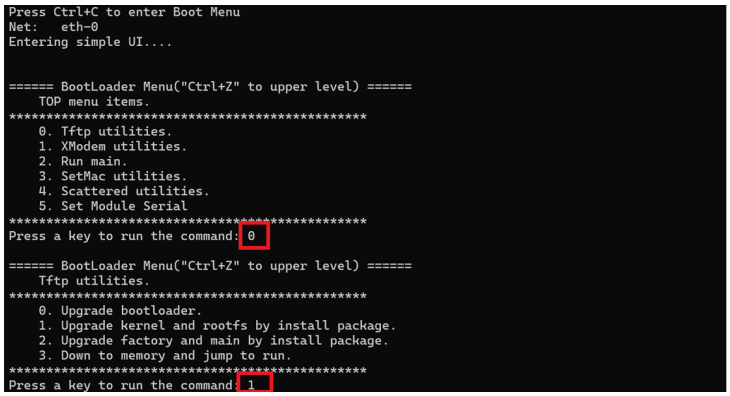
NOTE:

The installation package name for S3410 includes the suffix '**-rboot**', for example, **S3410-PicOS-4.4.5.14-2963b1e57b-rboot.bin**.

PICOS system can be installed under the Uboot menu through TFTP protocol for FS S3410 Series switches. The following steps describe the installation procedure.

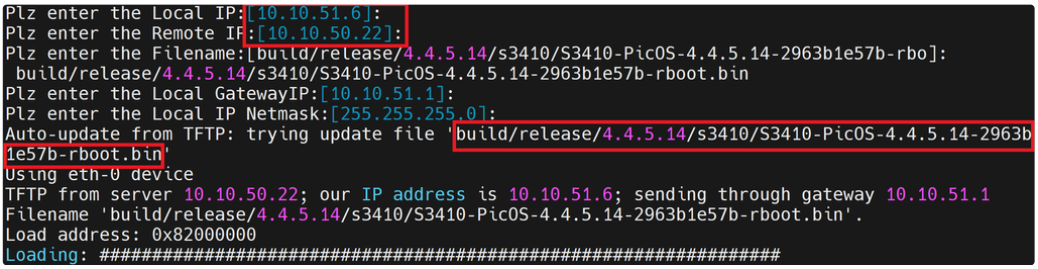
Step 1 Power off and on to force restarting the switch, then press **Ctrl+C** to enter Uboot menu.

Step 2 Enter **0** and then **1** in the Uboot menu to perform the installation process.



Step 3 Use TFTP protocol to download the installation files, and then install PICOS.

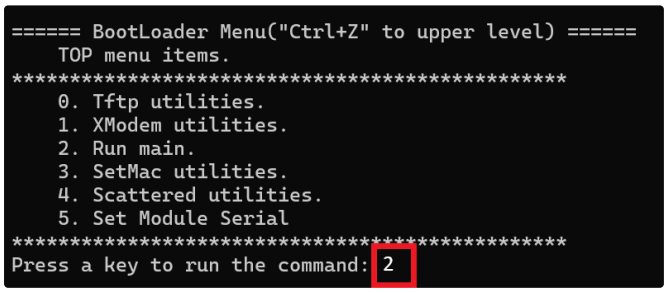
a) Configure the TFTP parameters. **Local IP** is the inband management interface IP of the switch, **Remote IP** is the IP of the TFTP server, **Filename** is the installation image directory and name located on the TFTP server.



b) After downloaded the installation image successfully, you need to input **Y** manually, then the system will automatically start system installation process.

c) Wait a few minutes before the installation process is completed. When **Success** is displayed, it indicates that the installation process is successfully completed.

Step 4 Press **Ctrl+Z** to go back to the Uboot menu, then type **2** to reboot the switch.



Then the device reboots and comes up running the new network operating system.

Users need to enter the username and password after the system restarts, the initial login username is **admin** and password is **pica8**. Then users will be asked to set a new password for admin. This is the only post installation step after which the PICOS operating system can be used.

Upgrading PICOS for FS S5810/S5860 Series Switches Using Upgrade Command (Login via Eth0 or Inband Management Interface)

- Preparation before Upgrading
  - Checking the Running PICOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data in Flash
  - Checking Available Flash Space
  - Upgrading Notes
- Upgrading Procedure
- Verifying Version after Upgrading

NOTE:

- This guide is only available for upgrading PICOS for FS S5810/S5860 Series switches when login via the **eth0** or **inband management interface**, and the supported version should be 4.4.5.7 or later versions before upgrade.
- During the upgrade process, the user connections and services will be interrupted. This means that users may lose access to the system, and any processes or transactions being handled by the services will be paused until the upgrade is complete. After the upgrade, users will need to reconnect to resume normal operations, and services will be restored.

Preparation before Upgrading

Table 1 Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build a different upgrade environment to get the upgrade software according to the need	
4	Getting the Required Upgrade Software	Obtain the required supporting upgrade software	
5	Backing up Important Data in Flash	All the important data in Flash is backed up	
6	Checking Available Flash Space	Flash space is enough to save upgrading package and other files	

Checking the Running PICOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
====================================
Base ethernet MAC Address     : 64:9d:99:d7:7d:23
Hardware Model                : S5860-48MG-U
Linux System Version/Revision : 4.4.5.7/4f6f523
Linux System Released Date    : 10/10/2024
L2/L3 Version/Revision        : 4.4.5.7/4f6f523
L2/L3 Released Date           : 10/10/2024
OVS/OF Version/Revision       : 4.4.5.7/4f6f523
OVS/OF Released Date          : 10/10/2024
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
{
"Type":"1GE",
"Feature":["Base Product", "Layer3", "OpenFlow"],
"Support End Date":"2020-10-28",
"Hardware ID":"ACD2-F77A-BBA3-2849",
"Site Name":"PICA8"
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment to get the upgrade software, the basic requirements are as follows:

- PC can log in to the device through eth0 or inband management interface.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following website for the latest version of upgrade software.

http://www.pica8.com/support/customer

Backing up Important Data in Flash

Before upgrading, save the important data (such as the configuration file) in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

> Where is the PicOS configuration?
>
> OVSDB file
>
> L2/L3 Configuration Files

Checking Available Flash Space

Use the **df** command to check the available flash space.

```
admin@PICOS:~$ df
Filesystem     1K-blocks   Used Available Use% Mounted on
udev              493028      0    493028   0% /dev
overlay           358904  57528    301376  17% /
tmpfs             512720      0    512720   0% /dev/shm
tmpfs             205088   3256    201832   2% /run
tmpfs               5120      0      5120   0% /run/lock
tmpfs              51200    292     50908   1% /tmp
/dev/ubi1_0       402660 208320    189500  53% /mnt/open
```

Upgrading Notes

- The device is not supported to upgrade to a previous version.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image can be modified during download, and the upgrade will fail during the md5 check.
- The image is platform dependent, that is, the image_name should be consistent with the platform, otherwise the upgrade script will abort.
- The image file is a **.bin** file, for example S5810-48TS-P-picos-e-4.4.5.7-2f6f578-fs.bin.
- Please find the log file related to PICOS upgrade process at */mnt/open/picos/config2/upgrade.log* and */mnt/open/picos/config1/upgrade.log*. This log file contains detailed information about the steps performed during the upgrade, including any errors or warnings that occurred. It can be used to troubleshoot issues or verify that the upgrade was completed successfully.
- When upgrading, the installer checks whether there is a user-data partition. If there exists a User-Data partition, the installer only rewrites the running system boot partition (PicOS/PicOS2) and installs the new installation package to this partition. However, if there is no User-Data partition, the installer removes all the partitions to rebuild a brand new NOS.
- Upgrade operation via upgrade commands is not allowed on non-default system, you can upgrade PICOS only on default system. When there are more than one PICOS, the default system is the one automatically booted into after system reboot.
- During the upgrade process, power interruption is not allowed.

Upgrading Procedure

NOTE :

Usage of **upgrade** command:

admin@PICOS:~$ sudo upgrade

USAGE

Upgrade system with local new image

SYNOPSIS

upgrade [image_name] [factory-default]

DESCRIPTION

image_name - Image with bin format file(*.bin)

factory-default - Recovery configuration to factory default

- PICOS upgrade is done via the command "**upgrade**" in bash (launching a shell script named "upgrade.sh"). This script will upgrade the image automatically.
- The file format of the upgrade package is ***.bin**.
- If there is an MD5 file in the /cftmp directory, the upgrade script will check package integrity with MD5. Else if there is no MD5 file in the /cftmp directory, then skip the MD5 check step.
- The option **factory-default** is used to reset the configuration to factory default when performing upgrade. This option retains the license files from the previous version.

The upgrading procedure in this document gives an example of upgrading on S5860-48MG-U from PICOS 4.4.5.7 to 4.4.5.8.

Step1 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5860/S5860_picos-4.4.5GA-7f06432992.bin  /cftmp
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5860/S5860_picos-4.4.5GA-7f06432992.bin.md5  /cftmp
```

NOTE:
If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:

admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5860/S5860_picos-4.4.5GA-7f06432992.bin /cftmp

admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5860/S5860_picos-4.4.5GA-7f06432992.bin.md5 /cftmp

If **sudo ip vrf exec mgmt-vrf** is not added, find the next-hop routing information from the default VRF. For the usage of VRF, refer to the VRF Configuration Guide.

Step2 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step3 Change directory to /cftmp.

```
admin@PICOS:~$ cd /cftmp
```

Step4 Run the **upgrade** command.

```
admin@PICOS:/cftmp$ sudo upgrade S5860_picos-4.4.5GA-7f06432992.bin
Upgrading system...
The connection may be interrupted. Please wait a moment to complete the upgrading procedure.
admin@PICOS:/cftmp$
```

NOTE :

- It will take about 5 minutes to finish upgrading PICOS. During the upgrade process, please be patient and do not perform any operation until the upgrade is complete, otherwise, the upgrade may be interrupted.
- During the upgrade process, the user connections and services will be interrupted. This means that users may lose access to the system, and any processes or transactions being handled by the services will be paused until the upgrade is complete.

Step5 After the upgrade, users will need to reconnect to resume normal operations, and services will be restored.

```
admin@PICOS:~$ ssh admin@10.10.51.54
```

Verifying Version after Upgrading

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address : d4:31:27:c9:e4:51
Hardware Model : S5860-48MG-U
Linux System Version/Revision : 4.4.5.8/7f06432992
Linux System Released Date : 10/14/2024
```

```
L2/L3 Version/Revision : 4.4.5.8/7f06432992
L2/L3 Released Date : 10/14/2024
OVS/OF Version/Revision : 4.4.5.8/7f06432992
OVS/OF Released Date : 10/14/2024
```

Upgrading PICOS by Using Upgrade2 for S5860 Series and S3410 Series Switches (Login via Eth0 or Inband Management Interface)

- Introduction
- Preparation before Upgrading
  - Checking the Running PICOS Version
  - Checking License Validation
  - Building Upgrade Environment
  - Getting the Required Upgrade Software
  - Backing up Important Data in Flash
- Upgrading Procedure
  - Upgrade2 Procedure
    - NOTE:
- Rollback Procedure
- Verifying Version after Upgrading

NOTE:

- This guide is only available for upgrading PICOS for FS S5860 Series and S3410 Series switches when login via the **eth0** or **inband management interface**, and the supported version should be 4.4.5.7 or later versions before upgrade.
- During the upgrade process, the user connections and services will be interrupted. This means that users may lose access to the system, and any processes or transactions being handled by the services will be paused until the upgrade is complete. After the upgrade, users will need to reconnect to resume normal operations, and services will be restored.
- The S3410 Series switches only support upgrade via the upgrade2 method.
- S5810 Series switches only support the **upgrade** method and do not support the **upgrade2** method.

Introduction

PICOS supports **upgrade2** method for system upgrade. There will be two separate systems on the device after the upgrade2 operation: PICOS and PICOS2. One of them will be the running system and the other will stay inactive. PICOS and PICOS2 system files and their respective configuration files are located in ***/mnt/open/picos/*** of the flash. A list and brief description of these files is as follows.

```
* uImage1.itb
* picos1.sqsh
* config1/backup_files              //User-defined backup files list
* config1/backup.tar.gz                  //Backup of latest.tar.gz
* config1/latest.tar.gz              //The newest configuration files
* uImage2.itb
* picos2.sqsh
* config2/backup_files
* config2/backup.tar.gz
* config2/latest.tar.gz
```

The upgrade2 installer installs the new system into the inactive system's file. The inactive system will be overwritten. After this operation, the new system is the inactive system and then the installer modifies the boot menu to make the newly installed system to be the default boot system. Finally, the system will come up running the new network operating system when boots up normally after the upgrading is finished,.

Upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system. This can reduce the network interruption risk due to the failure of system upgrade process and ensure the systems' continuous availability. You can refer to section Rollback Procedure for details.

We recommend using upgrade2 method to upgrade the NOS as there are functions of system backup and rollback.

Preparation before Upgrading

Table 1. Checklist before Upgrading

No.	Checking Items	Checking Standard	Results
1	Checking the Running PICOS Version	The currently running system software version is lower than the software version to be installed.	
2	Checking License Validation	Run the `license -s` command to verify that the license expiration date extends beyond the planned upgrade date. If the license is close to expiration, consider renewing it to avoid interruptions.	
3	Building Upgrade Environment	Build an upgrade environment to get the upgrade software according to the need.	
4	Getting the Required Upgrade Software	Obtain the required supporting upgrade software.	
5	Backing up Important Data in Flash	All the important data in Flash is backed up.	

Checking the Running PICOS Version

Use the **version** command to check the version of the running system software.

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
================================
Base ethernet MAC Address     : 64:9d:99:d7:7d:23
Hardware Model                : S5860-48MG-U
Linux System Version/Revision : 4.4.5.7/4f6f523
Linux System Released Date    : 10/10/2024
L2/L3 Version/Revision        : 4.4.5.7/4f6f523
L2/L3 Released Date           : 10/10/2024
```

```
OVS/OF Version/Revision       : 4.4.5.7/4f6f523
OVS/OF Released Date          : 10/10/2024
```

Checking License Validation

Before performing an upgrade, users can run the `license -s` command to check if the current license has expired, ensuring it is valid and preventing upgrade failure due to license expiration.

```
admin@PICOS:~$ license -s
{
"Type":"1GE",
"Feature":["Base Product", "Layer3", "OpenFlow"],
"Support End Date":"2020-10-28",
"Hardware ID":"ACD2-F77A-BBA3-2849",
"Site Name":"PICA8"
}
```

Building Upgrade Environment

Please make sure that you have set up an HTTP, TFTP or FTP protocol upgrading environment to get the upgrade software, the basic requirements are as follows:

- PC can log in to the device through SSH.
- The communication between the server and the device works well.
- The upgrading file used by the device has already been stored on the server.

Getting the Required Upgrade Software

Please contact Pica8 technical support engineers at the following website for the latest version of upgrade software.

http://www.pica8.com/support/customer

Backing up Important Data in Flash

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

Upgrading Notes

- Downgrade to an earlier version is NOT supported by using upgrade2 command.
- When using FTP/TFTP to download the image, user should verify that the "binary" mode is being used. If the "binary" transfer mode is not being used, the image can be modified during download, and the upgrade will fail during the md5 check.
- The image file is a **.bin** file, for example S5860-24XB-U-picos-e-4.4.5.7-2f6f578-fs.bin.
- Please find the log file related to PICOS upgrade process at */mnt/open/picos/config2/upgrade2.log* and */mnt/open/picos/config1/upgrade2.log.* This log file contains detailed information about the steps performed during the upgrade, including any errors or warnings that occurred. It can be used to troubleshoot issues or verify that the upgrade was completed successfully.
- The image is platform dependent, that is, the image_name should be consistent with the platform, otherwise the upgrade script will abort.
- During the upgrade process, power interruption is not allowed.

Upgrading Procedure

The upgrading procedure in this document gives an example of upgrading on S5860-48MG-U from 4.4.5.7 to 4.4.5.8 using **upgrade2** command.

> **NOTE：**
>
> Usage of **upgrade2** command:
>
> USAGE
>
> Upgrade system with local new image
>
> SYNOPSIS
>
> upgrade2 [image_name] [factory-default]
>
> DESCRIPTION
>
> image_name - Image with bin format file(*.bin)
> factory-default - Recovery configuration to factory default
>
> PICOS upgrade is done via the command "**upgrade2**" in bash (launching a shell script named "upgrade2.sh"). This script will upgrade the image and back up configuration files automatically.
>
> Image name is in the form of **.bin** from version 3.1.0, which should be copied to the /cftmp directory before running upgrade2 command.
>
> The **no-md5-check** option is removed from PICOS 3.1.0. If there is an MD5 file in the /cftmp directory, the upgrade script will check package integrity with MD5. Else if there is no MD5 file in the /cftmp directory, then skip the MD5 check step.
>
> The option **factory-default** is used to reset the configuration to factory default when performing upgrade, but it retains the license files from the previous version.

Upgrade2 Procedure

Step1 Copy the upgrade package (in the form of **.bin**) and the MD5 file to **/cftmp** directory by either FTP, TFTP, HTTP or SCP according to the actual upgrade environment. The following example uses the SCP method.

```
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5860/S5860_picos-4.4.5GA-7f06432992.bin  /cftmp
admin@PICOS:~$ sudo scp pica8@10.10.50.22:/tftp/build/daily/s5860/S5860_picos-4.4.5GA-7f06432992.bin.md5
/cftmp
```

> **NOTE:**
>
> If management VRF is enabled, and the FTP/TFTP/HTTP/SCP server is connected via the Eth0/1 port, you need to add the string **sudo ip vrf exec mgmt-vrf** before the SCP command when executing the scp operation. The format is as follows:
>
> admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5860/S5860_picos-4.4.5GA-7f06432992.bin /cftmp
>
> admin@PICOS:~$ sudo ip vrf exec mgmt-vrf scp pica8@10.10.50.22:/tftp/build/s5860/S5860_picos-4.4.5GA-7f06432992.bin.md5 /cftmp
>
> If **sudo ip vrf exec mgmt-vrf** is not added, find the next hop routing information from the default VRF. For the usage of VRF, refer to the VRF Configuration Guide.

Step2 Execute the **sync** operation.

```
admin@PICOS:~$ sync
```

Step3 Change directory to **/cftmp**.

```
admin@PICOS:~$ cd /cftmp
```

Step4 Run **upgrade2** command to begin upgrading.

```
admin@PICOS:/cftmp$ sudo upgrade2 S5860_picos-4.4.5GA-7f06432992.bin
Upgrading system...
The connection may be interrupted. Please wait a moment to complete the upgrading procedure.
admin@PICOS:/cftmp$
```

NOTE：

- It will take about 5 minutes to finish upgrading PICOS. During the upgrade process, please be patient and do not perform any operation until the upgrade is complete, otherwise, the upgrade may be interrupted.
- During the upgrade process, the user connections and services will be interrupted. This means that users may lose access to the system, and any processes or transactions being handled by the services will be paused until the upgrade is complete.

Step5 After the upgrade, users will need to reconnect to resume normal operations, and services will be restored.

```
admin@PICOS:~$ ssh admin@10.10.51.54
```

Rollback Procedure

The upgrade2 method supports system rollback function. The "**nos-rollback**" command can be used to revert to a previous version of the installed software package. Moreover, if it fails to upgrade, the system can automatically rollback to the old system.

NOTE：

Usage of **nos-rollback** command:

admin@PICOS:~$ sudo nos-rollback

USAGE

Rollback to the previous system after next reboot

SYNOPSIS

nos-rollback

The rollback procedure is as follows:

Step1 Run **nos-rollback** command for manually rollback.

```
admin@PICOS:~$ sudo nos-rollback
```

Step2 Reboot system manually to finish rollback.

```
admin@PICOS:~$ sudo reboot
```

You need to manually reboot the system after issued "**nos-rollback**" command and the system switching takes effect. After rebooting successfully, the system will come up running the previous version of network operating system.

Verifying Version after Upgrading

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address : d4:31:27:c9:e4:51
Hardware Model : S5860-48MG-U
Linux System Version/Revision : 4.4.5.8/7f06432992
Linux System Released Date : 10/14/2024
L2/L3 Version/Revision : 4.4.5.8/7f06432992
L2/L3 Released Date : 10/14/2024
OVS/OF Version/Revision : 4.4.5.8/7f06432992
OVS/OF Released Date : 10/14/2024
```

PICOS Debian Package Upgrade User Guide

- Overview
- How to use
- Verifying after Upgrade
- Appendix

Overview

PICOS provides five Debian packages from release 3.2 to let users upgrade some of the available components manually, or reinstall PICOS components in case some of them were broken.

Available PICOS Debian packages and the dependencies between them are described below:

- picos-linux

  PICOS Linux Kernel, drivers and switching ASIC kernel modules

- picos-vasic
  - PICOS VASIC and line card management libraries and utilities
  - Depends on picos-linux
- picos-xorplus
  - PICOS Layer 2 and Layer 3 software package
  - Depends on picos-vasic, picos-utils
- picos-ovs
  - PICOS OVS package
  - “picos-ovs” will have its own lib to access peripherals (such as FAN and PSU and LED) via sysfs
  - Depends on picos-vasic, picos-utils
- picos-utils
  - PICOS common utilities and configuration files
  - System config files, systemd units
  - Common utility such as ZTP/diag

In this way, we do not need to upgrade the entire PICOS system if version changes only appear in one or several of the components. This provides an efficient and effective method of upgrading PICOS system.

> **NOTE：**
>
> Some PICOS component packages would depend on other parts, so the dependent ones should be installed first if they do not exist on the system.

How to use

When new releases of PICOS components have been made available to fix urgent issues, users can get the Debian packages from PICOS support team.

For example, the package users get might be "picos-xorplus-s4100-3.2.3-9dc8d94.deb" saved in the working directory.

To install the package, the following command is OK:

```
admin@Xorplus:~$ sudo dpkg -i picos-xorplus-s4100-3.2.3-9dc8d94.deb
```

After finishing upgrade, the switch will reboot automatically, the system will come up running the PICOS operating system with the new PICOS component.

> **NOTE：**
>
> If certain PICOS components have been removed from the running Linux system, this operation would be an installation instead of upgrade. In this case, users need to confirm the model compatibility manually by inputting `Yes` or `Y` at the prompt `Are you sure the model is *MODEL* (yes/no)?`

Verifying after Upgrade

We can use the following command to check the status of PICOS Debian packages after upgrade.

```
admin@Xorplus:~$ dpkg -l | grep picos-
ii  picos-linux
ii  picos-ovs
ii  picos-utils
ii  picos-vasic
ii  picos-xorplus
```

Here two "**i**" represent **normal**, the first one indicates that the package has been installed successfully. The second "**i**" indicates the installation dependencies between the components and configuration operations are successfully completed met.

Appendix

PICOS component package uninstall operation is provided as follows.

> **NOTE：**
>
> - Uninstall the PICOS component packages may cause severe system errors, we strongly recommend not to uninstall any of the PICOS component package.
> - The uninstall operation will uninstall all packages that depend on this package, either directly or indirectly.

```
admin@Xorplus:~$ sudo apt remove picos-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  picos-utils
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n]
```

Zero Touch Provisioning (ZTP)

- Overview of ZTP
  - ZTP Fundamentals
  - DHCP Configuration of ZTP
  - Provision Script
- Enabling or Disabling ZTP
- Preparation before ZTP Deployment
- Example for Implementing ZTP Deployment through DHCP
- Appendix: ZTP API

Overview of ZTP

- ZTP Fundamentals
- DHCP Configuration of ZTP
- Provision Script

ZTP Fundamentals

NOTEs:

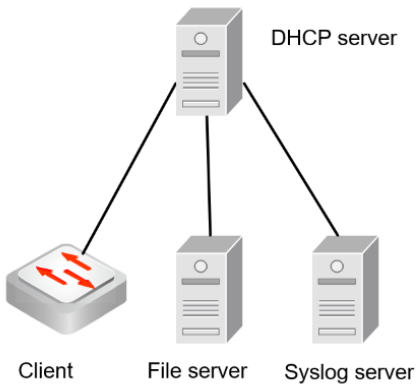
- Currently, the IPv6 ZTP is not supported.
- You are suggested to implement ZTP for unconfigured devices, or the error prompts may appear.
- Before using ZTP, you should configure the switch with two partitions of active partition and backup partition. The active partition can be used for upgrade and the backup partition can be used to save the current version, which can make sure the original version can be recovered once the upgrade is failed.

ZTP (Zero Touch Provisioning) is a technology for automated upgrade and configuration of unconfigured network devices. You can automatically upgrade and configure devices with the provision script of ZTP before the PicOS is up, obtaining the required configuration information without manual intervention, including IP addresses, routing, security policies, etc.

When large numbers of switches need to be upgraded to new versions or issued with configuration files, you can use ZTP to reduce labor costs and improve deployment efficiency. It can implement fast, accurate and reliable device deployment.

Typical Network

Figure 1. Typical network of ZTP

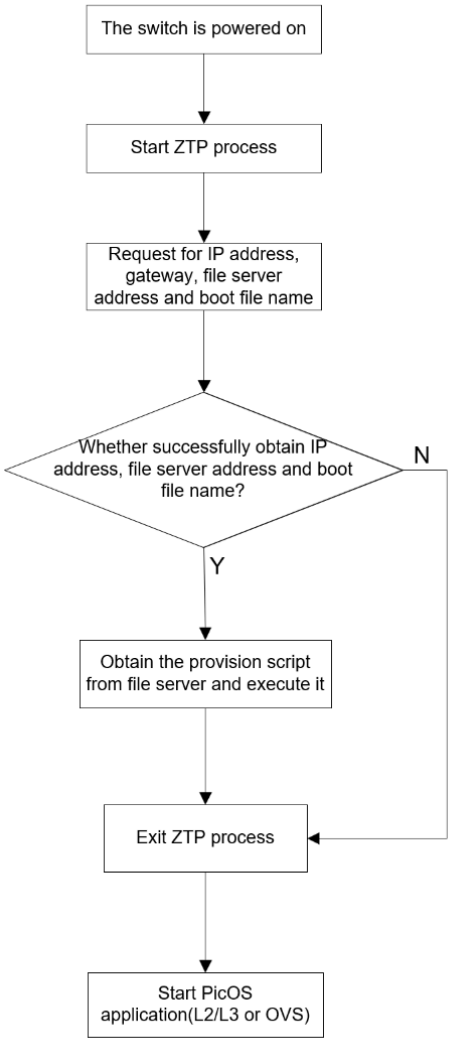


The typical network of ZTP is shown as Figure1. The switch is served as the DHCP client, which uses information configured on the provision script or the DHCP server to locate necessary files on the file server, and sends logs to the Syslog server. The details of device role are shown as below:

- **DHCP client**: the switch can be configured as DHCP client. By default, the client function of management interface eth0 (or VLAN 1 without eth0) is enabled, and the IP address assigned by DHCP server is configured for the management interface, which can be used to communicate with the file server.
- **DHCP server**: allocates the management IP address, default gateway address, file server address and Syslog server address to clients.
- **File server (TFTP server or HTTP server)**: stores the files as needed, such as provision script, configuration file and software image. You can obtain these files from FS support stuffs. For detailed information of configuring TFTP server or HTTP server, see the third-party information.
- **Syslog server**: Optional. It is required only when the switch need to send logs to the Syslog server.

ZTP Process

Figure 2. ZTP process



The ZTP process is shown as above:

1. The switch (DHCP client) is powered on and starts ZTP process.
2. The client sends DHCP request packets to the DHCP server periodically to obtain the management IP address, gateway, file server IP address, boot file name and syslog server IP address. The DHCP server responds with the DHCP ACK packets containing the above information. The interaction is based on DHCP options, see Option Parameters.

> If the client cannot successfully obtain the management IP address, file server address or boot file name, the switch will exit ZTP process.

3. According to the above information, the switch obtains provision script from the file server and execute it. You can customize the script contents by running the *generate_script*, see Provision Script.
4. The switch starts PicOS application (L2/L3 or OVS).

DHCP Configuration of ZTP

Option Parameters

The DHCP server obtains network configuration information required by ZTP through option parameters. The request packets sent by DHCP client carry option 55, and the reply packets responded by DHCP server carry option 7, 66 and 67. The function of option parameters is shown as below.

Table 1. Option description

Option	Description	Carrier
55	Specifies the network configuration parameters need to be obtained from the server. It includes the boot file name, TFTP server address, Syslog server address and gateway.	Client
7	Specifies the IP address of Syslog server.	Server
66	Specifies the IP address of TFTP(HTTP) server allocated for the client.	Server
67	Specifies the boot file name allocated for the client.	Server

DHCP Server Configuration

When the switch is served as the DHCP server, you can configure the DHCP server through PicOS commands (**suggested**) or Linux commands.

PicOS command

Here is an example of configuring the DHCP server through PicOS commands, which specifies the IP address of Syslog server as 192.168.10.1, the IP address of TFTP server as 192.168.10.1, and the working path of provision script on the TFTP server as *./provision.sh*. For detailed information of related commands, see Configuring DHCP server.

```
admin@PICOS# set protocols dhcp server pool pool1 log-server 192.168.10.1
admin@PICOS# set protocols dhcp server pool pool1 tftp-server 192.168.10.2
admin@PICOS# set protocols dhcp server pool pool1 bootfile-name file-path ./provision.sh
admin@PICOS# commit
```

Linux command

Here is an example of configuring the DHCP server through Linux commands.

```
host pica8-pxxxx
{************************//////////////////////////////////////////////////////////////////////////////////
///
hardware ethernet 08:9e:01:62:d5:62;
option bootfile-name "pica8/provision.script";
option tftp-server-name "xx.xx.xx.xx";
option log-servers xx.xx.xx.xx;
fixed-address xx.xx.xx.xx;
}
```

The elements of the segment above are described below:

- **host:** the host name of the PicOS switch.
- **hardware ethernet:** the MAC address of the PicOS switch.
- **bootfile-name:** the file name of the shell scripts and its path relative to the TFTP root directory.
- **tftp-server-name:** the IP address of the TFTP server.
- **log-servers:** the IP address of the log server that will receive logs from ZTP.
- **fixed-address:** optional. Configure a fixed IP address as management IP of the switch.

PicOS switches send a *vendor-class-identifier* to the DHCP server in the format of *pica8-pxxxx* where *xxxx* is the switch model. It is possible for the customer to use the *vendor-class-identifier* to identify PicOS switches.

Provision Script

The provision script describes what is required and how to execute when you upgrade and configure PicOS through ZTP. You can customize the provision script through running the *generate_script* file. The *generate_script* is provided in the format of Shell and Python, and you can click generate_script.py or generate_script.sh to download. The detailed contents are shown as below.

Generate Script in the Shell Format

Shell Script Content

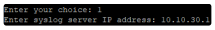
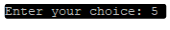
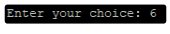
```
#!/bin/bash

function prompt_choice() {
    echo "Please choose an option to configure (enter the number to select, enter 'done' to generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file \"picos_start.conf\" from file server
    9. Get PicOS configuration file \"pica_startup.boot\" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file \"ovs-vswitchd.conf.db\" from file server"
    read -rp "Enter your choice: " choice
}

function generate_script() {
    local config_commands=()
    local revision=""
    while true; do
        prompt_choice

        case $choice in

            1)
                read -rp "Enter syslog server IP address: " ip
                config_commands+=("add_remote_syslog_server $ip")
                ;;
            2)
                read -rp "Enter the syslog server IP address to remove: " ip
                config_commands+=("remove_remote_syslog_server $ip")
                ;;
            3)
                read -rp "Enter file name in TFTP server: " remote_file_name
                read -rp "Enter file name with path in local: " local_file_name
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("tftp_get_file $remote_file_name $local_file_name $ip")
                ;;
            4)
                read -rp "Enter file name with path in local: " local_file_name
                read -rp "Enter file name with HTTP server URL: " file_name
```

```
                config_commands+=("http_get_file $local_file_name $file_name")
                ;;
            5) config_commands+=("ztp_enable") ;;
            6) config_commands+=("ztp_disable") ;;
            7)
                read -rp "Enter tftp file name or http url: " file_name
                read -rp "Enter the software revision of the image:" revision
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("if [ \"\$revision\" != \"$revision\" ]; then get_picos_image $file_name $ip; fi")
                ;;
            8)
                read -rp "Enter tftp file name or http url: " file_name
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("get_picos_startup_file $file_name $ip")
                ;;
            9)
                read -rp "Enter tftp file name or http url: " file_name
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("get_l2l3_config_file $file_name $ip")
                ;;
            10)
                read -rp "Enter tftp file name or http url: " file_name
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("l2l3_load_config $file_name $ip")
                ;;
            11)
                read -rp "Enter tftp file name or http url: " file_name
                read -rp "Enter TFTP server IP address (optional): " ip
                config_commands+=("get_ovs_config_file $file_name $ip")
                ;;
            done)
                break
                ;;
            *)
                echo "Invalid choice, please try again."
                ;;
        esac
        printf "\n"
    done

    # Generate Shell script
    local script_name="provision.sh"
    {
        echo "#!/bin/bash"
        echo "source /usr/bin/ztp-functions.sh"
        echo ""
        for command in "${config_commands[@]}"; do
            echo "$command"
        done
    } > "$script_name"
    printf "\n"
    echo "Generated Shell script has been saved as $script_name"
}

# Run script generation program
generate_script
```

Option Description of Shell Script

NOTEs:

- Make sure that names of all files configured in the script is the same with files placed in the file server, or the switch cannot obtain them successfully.
- The IP address of TFTP server from DHCP server will be valid if it is not configured in the script.

Option	Description	Example
1. Add remote Syslog server	Specify the IPv4 address of the Syslog server.	 The IPv4 address of Syslog server is configured as *10.10.30.1*.
2. Remove remote Syslog server	Delete the IPv4 address of the Syslog server.10.10.30.1	 The IPv4 address *10.10.30.1* of Syslog server is deleted.
3. Get file from TFTP server	Download a file with specified name from the TFTP server with a specified IP address and path, and save it in local with another specified name. The path */cftmp* is valid if you don't specify the local path here.	 The file *remote-file.txt* in the TFTP server *10.10.30.2* is downloaded and is saved in local as *local-file.txt*.
4. Get file from HTTP server	Download a file with specified name from the HTTP server with a specified URL and save it in local with another specified name. The root path is valid if you don't specify the local path here.	 The file *remote-file.txt* in the HTTP server *10.10.30.2* is downloaded and is saved in local as *local-file.txt*.
5. Enable ZTP auto-run when switch boot up	Enable ZTP function after completing this ZTP process. You are suggested to configure this option at last, or it may be invalid.	
6. Disable ZTP auto-run when switch boot up	Disable ZTP function after completing this ZTP process. You are suggested to configure this option at last, or it may be invalid.	
7. Get PicOS image from file server and upgrade	Download the PicOS image from the TFTP server with the specified IP address, path and name, or from the HTTP server with URL. Then, upgrade the switch to the new version.	 The image *onie-installer-picos-9.8.7-main-43d73dd983-x86v.bin* in the working path of the TFTP server *10.10.30.2* is downloaded, and the switch is upgraded to this new version with the version number *43d73dd983*.

	• You should specify the version number to make sure the switch only upgrades one time. • You don't need to configure the TFTP server IP address when downloading files from the HTTP server.	
8. Get PicOS startup file "picos_start.conf" from file server	Download the PicOS startup file *picos_start.conf* from the TFTP server with the specified IP address, path and name, or from the HTTP server with URL. You don't need to configure the TFTP server IP address when downloading files from the HTTP server.	 The file *picos_start.conf* from the HTTP server *10.10.30.3* is downloaded.
9. Get PicOS configuration file "pica_startup.boot" from file server	Download the L2/l3 configuration file *pica_startup.boot* from the TFTP server with the specified IP address, path and name, or from the HTTP server with URL. You don't need to configure the TFTP server IP address when downloading files from the HTTP server.	 The file *pica_startup.boot* from the HTTP server *10.10.30.3* is downloaded.
10. Get file with PicOS L2/L3 CLI commands list and execute these commands	Download the L2/l3 command file from the TFTP server with the specified IP address, path and name, or from the HTTP server with URL. • You don't need to configure the TFTP server IP address when downloading files from the HTTP server. • You can modify the file *ztpl2l3_cfg.cli* as needed. For example, if you need to specify	 The file *ztpl2l3_cfg.cli* in the working directory of the TFTP server *10.10.30.2* is downloaded.

	VLAN 10 and VLAN 20, you can configure as follows:
	`set vlans vlan-id 20`
	`set vlans vlan-id 30`	

11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file server	Download the OVS configuration file *ovs-vswitchd.conf.db* from the TFTP server with the specified IP address, path and name, or from the HTTP server with URL. You don't need to configure the TFTP server IP address when downloading files from the HTTP server.	 The file *ovs-vswitchd.conf.db* from the HTTP server *10.10.30.3* is downloaded.

Generate Script in the Python Format

Python Script Content

```
import os
def prompt_choice():
    print("""Please choose an option to configure (enter the number to select, enter 'done' to generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file server""")
    return input("Enter your choice: ")

def generate_script():
    config_commands = []

    while True:
        choice = prompt_choice()

        if choice == 'done':
            break

        if choice == '1':
            ip = input("Enter syslog server IP address: ")
            config_commands.append(f"add_remote_syslog_server {ip}")
```

```
        elif choice == '2':
            ip = input("Enter the syslog server IP address to remove: ")
            config_commands.append(f"remove_remote_syslog_server {ip}")
        elif choice == '3':
            remote_file_name = input("Enter file name in TFTP server: ")
            local_file_name = input("Enter file name with path in local: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f"tftp_get_file {remote_file_name} {local_file_name} {ip}")
        elif choice == '4':
            local_file_name = input("Enter file name with path in local: ")
            file_name = input("Enter file name with HTTP server URL:: ")
            config_commands.append(f"http_get_file {local_file_name} {file_name}")
        elif choice == '5':
            config_commands.append("ztp_enable")
        elif choice == '6':
            config_commands.append("ztp_disable")
        elif choice == '7':
            file_name = input("Enter tftp file name or http url: ")
            revision = input("Enter the software revision of the image: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f'if [ "$revision" != "{revision}" ]; then get_picos_image {file_name}
{ip}; fi')
        elif choice == '8':
            file_name = input("Enter tftp file name or http url: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f"get_picos_startup_file {file_name} {ip}")
        elif choice == '9':
            file_name = input("Enter tftp file name or http url: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f"get_l2l3_config_file {file_name} {ip}")
        elif choice == '10':
            file_name = input("Enter tftp file name or http url: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f"l2l3_load_config {file_name} {ip}")
        elif choice == '11':
            file_name = input("Enter tftp file name or http url: ")
            ip = input("Enter TFTP server IP address (optional): ")
            config_commands.append(f"get_ovs_config_file {file_name} {ip}")
        else:
            print("Invalid choice, please try again.")

        print("\n")

    # Generate Shell script
    script_name = "provision.sh"
    with open(script_name, 'w') as script_file:
        script_file.write("#!/bin/bash\n")
        script_file.write("source /usr/bin/ztp-functions.sh\n")
        script_file.write("\n")
        for command in config_commands:
            script_file.write(f"{command}\n")

    print(f"\nGenerated Shell script has been saved as {script_name}")

# Run script generation program
generate_script()
```

Option Description of Python Script

The description of the Python script is the same with the Shell script. For detailed information, see Option Description of Shell Script.

Configuration Example for Generating Provision.sh

Take the Shell script as an example to introduce how to use it:

1. Upload the Shell script *generate_script.sh* to the Linux environment.
2. Use the command **chmod +x *generate_script.sh*** to enable the executable permission.
3. Enter command ***./generate_script.sh*** to run the script, and options are shown as below.

```
admin@PICOS:~$ chmod +x generate_script.sh
admin@PICOS:~$ ./generate_script.sh
Please choose an option to configure (enter the number to select, enter 'done' to generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file server
```

4. Select options of 1, 3 and 6 in sequence as needed, and enter **done** to generate the script.

```
Please choose an option to configure (enter the number to select, enter 'done'
o generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file serve
Enter your choice: 1
Enter syslog server IP address: 192.168.1.100

Please choose an option to configure (enter the number to select, enter 'done'
o generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file serve
Enter your choice: 3
Enter file name in TFTP server: remote-file.txt
Enter file name with path in local: local-file.txt
Enter TFTP server IP address (optional): 192.168.1.101

Please choose an option to configure (enter the number to select, enter 'done'
o generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file serve
Enter your choice: 6

Please choose an option to configure (enter the number to select, enter 'done'
o generate the script):
    1. Add remote Syslog server
    2. Remove remote Syslog server
    3. Get file from TFTP server
    4. Get file from HTTP server
    5. Enable ZTP auto-run when switch boot up
    6. Disable ZTP auto-run when switch boot up
    7. Get PicOS image from file server and upgrade
    8. Get PicOS startup file "picos_start.conf" from file server
    9. Get PicOS configuration file "pica_startup.boot" from file server
   10. Get file with PicOS L2/L3 CLI commands list and execute these commands
   11. Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file serve
Enter your choice: done

Generated Shell script has been saved as provision.sh
```

5. The file named *provision.sh* is generated in the current directory, which includes all selected options. The content of provision script is shown as below.

```
admin@PICOS:~$ cat provision.sh
#!/bin/bash
source /usr/bin/ztp-functions.sh

add_remote_syslog_server 192.168.1.100
tftp_get_file remote-file.txt local-file.txt 192.168.1.101
ztp_disable
```

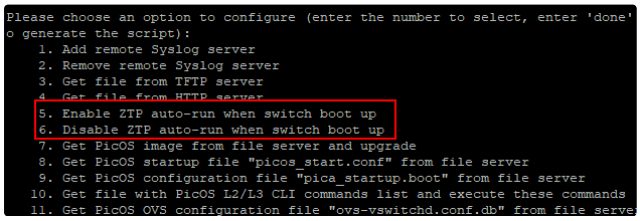
Enabling or Disabling ZTP

NOTE:

By default, ZTP is enabled on PicOS switches. If ZTP is left enabled, the PicOS switch will try to download a new script every time the switch is booted. This is not a desirable situation, so ZTP should be disabled when it is no longer needed.

Four methods are supported to disable or enable ZTP, as detailed below:

- Enable or disable ZTP through running the provision script. To generate the corresponding provision script, select options of 5 and 6 when running the *generate_script*, as shown below.



you are suggested to select this option at last, or the option may be invalid.

- Enable or disable ZTP through the command **set system ztp enable** <**true** | **false**> in PICOS configuration mode. The following example disables ZTP using the command **set system ztp enable** <**true** | **false**>:

```
dmin@XorPlus# set system ztp enable false
admin@XorPlus# commit
```

- Enable or disable ZTP via the **ztp-config** script included with PicOS. The following example disables ZTP using the **ztp-config** script run from the Linux shell:

```
admin@LEAF-A$sudo ztp-config
Please configure the default PicOS ZTP options:
    (Press other key if no change)
         [1]  PicOS ZTP enabled   * default
         [2]  PicOS ZTP disabled
Enter your choice (1,2):2
PicOS ZTP is disabled.
admin@LEAF-A$
```

- Manually edit the PicOS configuration file **picos_start.conf** and change the value of the **ztp_disable** variable. The following snippet from the PicOS configuration file shows that ZTP has been disabled (**ztp_disable**=**true**).

```
admin@LEAF-A$more /etc/picos/picos_start.conf | grep ztp
ztp_disable=true
```

To enable ZTP, you need to set **ztp_disable** to **false**.

Preparation before ZTP Deployment

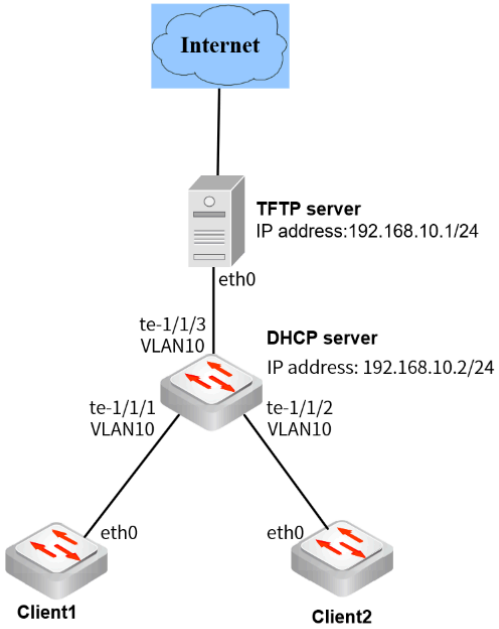
Before powering on the switch to start ZTP deployment, you should make the following preparations:

Items	Preparations
DHCP client	It is network reachable, which can communicate with the DHCP server and file server.
File server	It is configured successfully and is network reachable.
DHCP server	It is network reachable. If the switch is served as the server, you should configure the IP address of file server, the path and name of provision script and the IP address of Syslog server (optional).
Required files	Obtain files (image file, L2/L3 configuration file, OVS configuration file, L2/L3 command file or startup file) from FS stuffs, and save them in the working directory of file servers. **Note**: the *provision.sh* is generated through running the *generate_script* file. For details, see Configuration Example for Generating Provision.sh.

Example for Implementing ZTP Deployment through DHCP

Overview

Figure 1. Typical topology of ZTP implementation



In **Figure 1**, switches are configured respectively as the DHCP client and DHCP server. The client uses information configured on a DHCP server to locate the software image and configuration files on the TFTP server, and then download specified files to upgrade system and load configurations.

The data plan is shown as below:

Device	Interface	VLAN and IP Address
DHCP server	te-1/1/1 te-1/1/2 te-1/1/3	VLAN: 10 IP address: 192.168.10.2/24
TFTP server	eth0	IP address: 192.168.10.1/24

The image information of Client1 and Client2, and the files to be loaded are shown as below:

Device	Current version	Files to be loaded
Client1	PicOS-9.8.7	Image: PICOS-9.8.7-main-43d73dd983-x86v.bin
Client2	PicOS-4.4.0	Command file: ztpl2l3_cfg.cli

Procedure

DHCP Server

Step 1 Configure VLAN and interface.

```
admin@PICOS# set vlans vlan-id 10
admin@ PICOS # set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@ PICOS # set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 10
admin@ PICOS # set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 10
admin@ PICOS # set vlans vlan-id 10 l3-interface vlan10
admin@ PICOS # set l3-interface vlan-interface vlan10 address 192.168.10.2 prefix-length 24
admin@ PICOS # commit
```

Step 2 Configure DHCP pool.

```
admin@PICOS# set protocols dhcp server pool pool1 network address 192.168.10.2 prefix-length 24
admin@PICOS# set protocols dhcp server pool pool1 lease-time 1440
admin@ PICOS # set protocols dhcp server pool pool1 range range1 low 192.168.10.3
admin@ PICOS # set protocols dhcp server pool pool1 range range1 high 192.168.10.20
admin@ PICOS # set protocols dhcp server pool pool1 tftp-server 192.168.10.1
admin@ PICOS # set protocols dhcp server pool pool1 bootfile-name file-path provision.sh
admin@ PICOS # set ip routing enable true
admin@ PICOS # commit
```

TFTP Server

Step 1 Set the basic configuration of TFTP server.

Make sure that the TFTP server is network reachable, which can communicate with the DHCP server and DHCP client.

Step 2 Configure files needed to be saved in the TFTP server.

- For the provision file *provision.sh*, you need to run *generate_script* with options 7 and 10 selected to generate it. For details, see Option Description of Shell Script.
- For the L2/L3 command file *ztpl2l3_cfg.cli,* you can modify it as needed, such as configuring VLAN20 and VLAN30.

Step 3 Save the image file, provision script and L2/L3 command file to the working path of TFTP server.

The working path of TFTP server here is */home/admin/tftp*, and you should modify it based on the actual circumstances.

Step 4 Generate the MD5 file.

Enter the directory which saves image file, and run the following Linux command to generate MD5 file. The generated MD5 file will be saved in this directory.

The MD5 file name must be the format of *image-file-name.md5*, otherwise the DHCP server cannot recognize it.

```
admin@TFTP:~$ cd /home/admin/tftp
admin@TFTP:~/tftp$ md5sum onie-installer-picos-9.8.7-main-43d73dd983x86v.bin > onie-installer-picos-9.8.7-main-43d73dd983-x86v.bin.md5
```

Step 5 View the files saved in the directory of */home/admin/tftp*.

```
admin@PICOS:~$ ls /home/admin/tftp
```

```
admin@PICOS:~$ ls /home/admin/tftp/
onie-installer-picos-9.8.7-main-43d73dd983x86v.bin      provision.sh
onie-installer-picos-9.8.7-main-43d73dd983x86v.bin.md5  ztpl2l3_cfg.cli
```

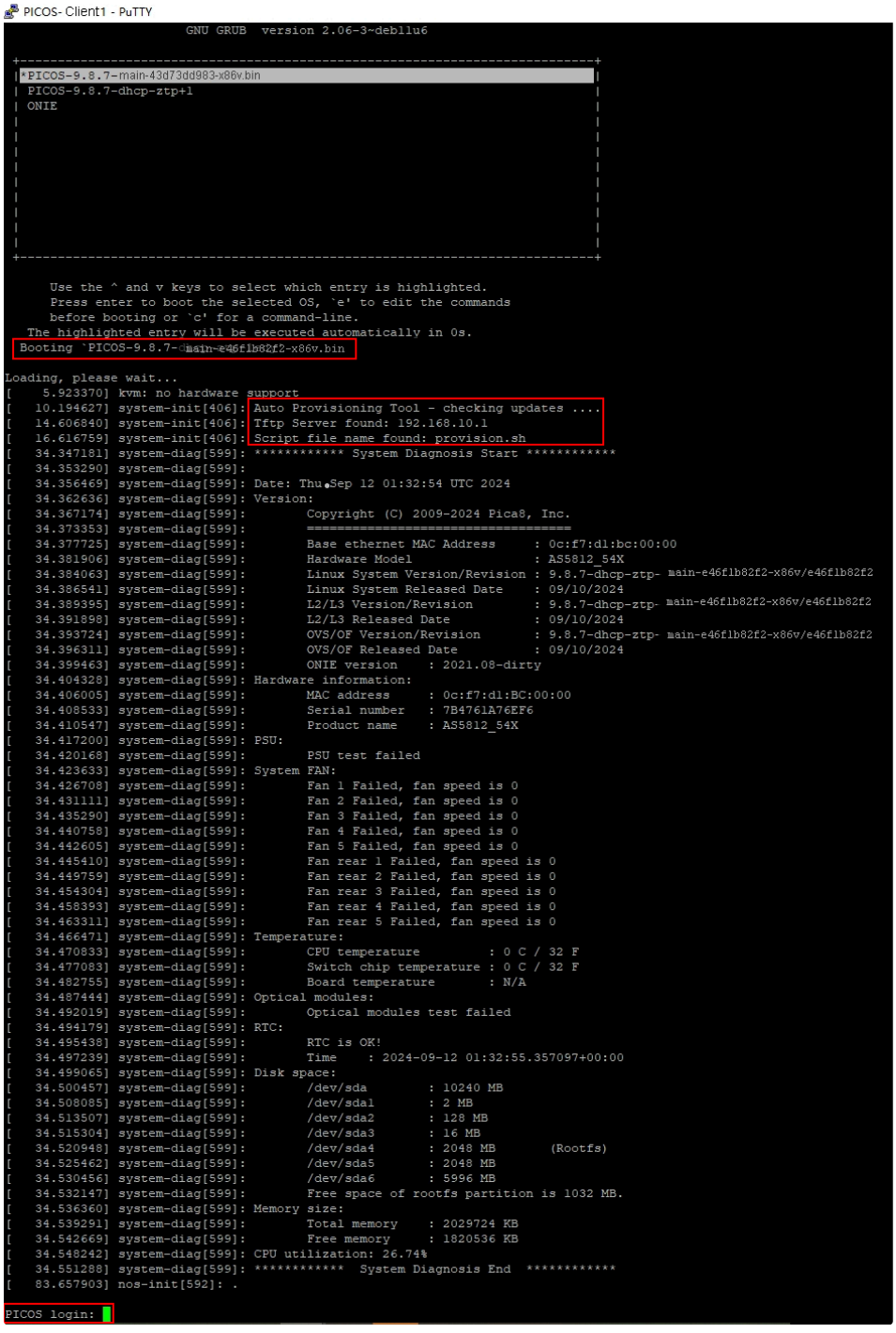
DHCP Client

After completing the above configuration, start client1 and client2.

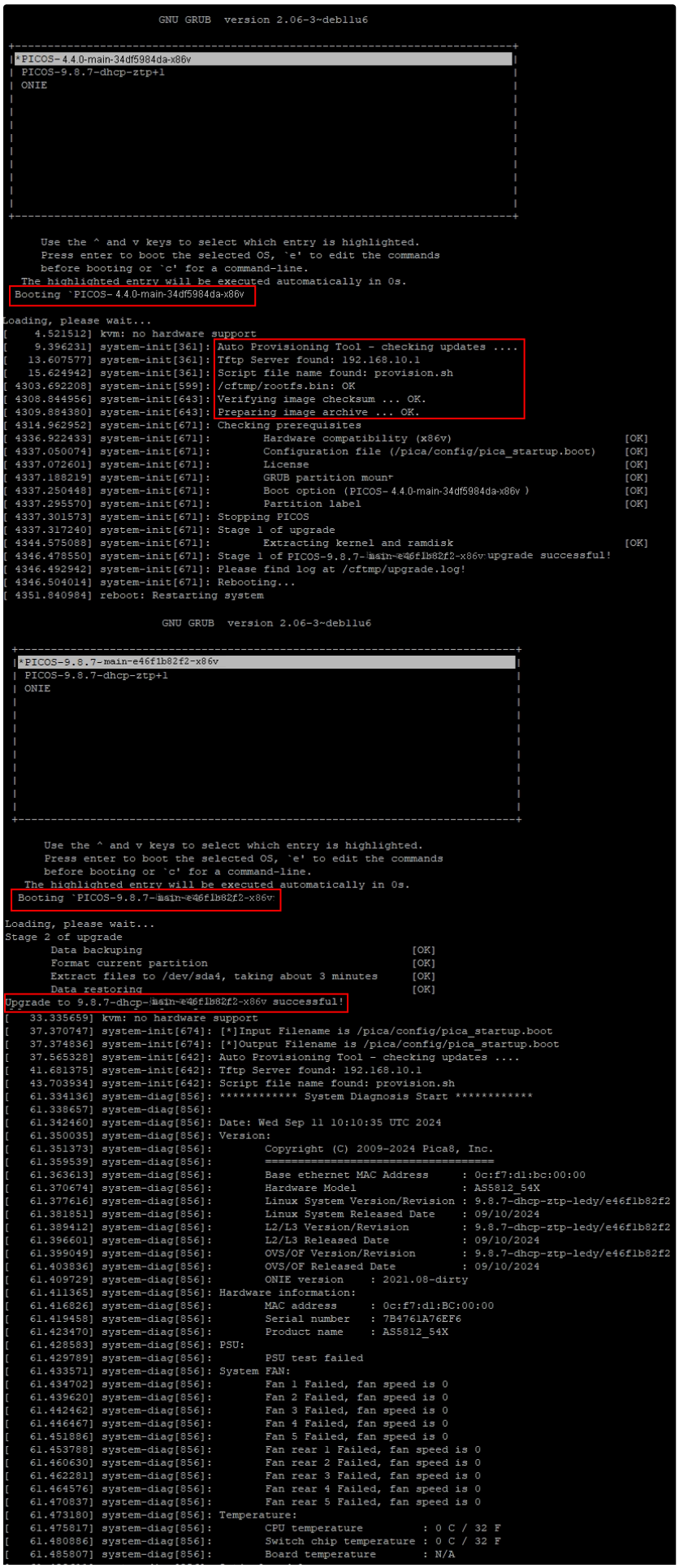
Verifying the Configuration

- View the upgrade process of client1 and client2.

Client1: for the version is already V9.8.7, it directly loads L2/L3 command configurations.



Client2: for the version is V4.4.0, it upgrades to V9.8.7 and then loads L2/L3 command configurations.


GNU GRUB version 2.06-3~deb11u6
*PICOS- 4.4.0-main-34df5984da-x86v
PICOS-9.8.7-dhcp-ztp+1
ONIE
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 0s.
Booting `PICOS- 4.4.0-main-34df5984da-x86v
Loading, please wait...
[4.521512] kvm: no hardware support
[9.396231] system-init[361]: Auto Provisioning Tool - checking updates ....
[13.607577] system-init[361]: Tftp Server found: 192.168.10.1
[15.624942] system-init[361]: Script file name found: provision.sh
[4303.692208] system-init[599]: /cftmp/rootfs.bin: OK
[4308.844956] system-init[643]: Verifying image checksum ... OK.
[4309.884380] system-init[643]: Preparing image archive ... OK.
[4314.962952] system-init[671]: Checking prerequisites
[4336.922433] system-init[671]: Hardware compatibility (x86v) [OK]
[4337.050074] system-init[671]: Configuration file (/pica/config/pica_startup.boot) [OK]
[4337.072601] system-init[671]: License [OK]
[4337.188219] system-init[671]: GRUB partition mount [OK]
[4337.250448] system-init[671]: Boot option (PICOS- 4.4.0-main-34df5984da-x86v) [OK]
[4337.295570] system-init[671]: Partition label [OK]
[4337.301573] system-init[671]: Stopping PICOS
[4337.317240] system-init[671]: Stage 1 of upgrade
[4344.575088] system-init[671]: Extracting kernel and ramdisk [OK]
[4346.478550] system-init[671]: Stage 1 of PICOS-9.8.7-main-e46f1b82f2-x86v upgrade successful!
[4346.492942] system-init[671]: Please find log at /cftmp/upgrade.log!
[4346.504014] system-init[671]: Rebooting...
[4351.840984] reboot: Restarting system
GNU GRUB version 2.06-3~deb11u6
*PICOS-9.8.7-main-e46f1b82f2-x86v
PICOS-9.8.7-dhcp-ztp+1
ONIE
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 0s.
Booting `PICOS-9.8.7-main-e46f1b82f2-x86v
Loading, please wait...
Stage 2 of upgrade
Data backuping [OK]
Format current partition [OK]
Extract files to /dev/sda4, taking about 3 minutes [OK]
Data restoring [OK]
Upgrade to 9.8.7-dhcp-main-e46f1b82f2-x86v successful!
[33.335659] kvm: no hardware support
[37.370747] system-init[674]: [*]Input Filename is /pica/config/pica_startup.boot
[37.374836] system-init[674]: [*]Output Filename is /pica/config/pica_startup.boot
[37.565328] system-init[642]: Auto Provisioning Tool - checking updates ....
[41.681375] system-init[642]: Tftp Server found: 192.168.10.1
[43.703934] system-init[642]: Script file name found: provision.sh
[61.334136] system-diag[856]: ************ System Diagnosis Start ************
[61.338657] system-diag[856]:
[61.342460] system-diag[856]: Date: Wed Sep 11 10:10:35 UTC 2024
[61.350035] system-diag[856]: Version:
[61.351373] system-diag[856]: Copyright (C) 2009-2024 Pica8, Inc.
[61.359539] system-diag[856]: ==========
[61.363613] system-diag[856]: Base ethernet MAC Address : 0c:f7:d1:bc:00:00
[61.370674] system-diag[856]: Hardware Model : AS5812_54X
[61.377616] system-diag[856]: Linux System Version/Revision : 9.8.7-dhcp-ztp-ledy/e46f1b82f2
[61.381851] system-diag[856]: Linux System Released Date : 09/10/2024
[61.389412] system-diag[856]: L2/L3 Version/Revision : 9.8.7-dhcp-ztp-ledy/e46f1b82f2
[61.396601] system-diag[856]: L2/L3 Released Date : 09/10/2024
[61.399049] system-diag[856]: OVS/OF Version/Revision : 9.8.7-dhcp-ztp-ledy/e46f1b82f2
[61.403836] system-diag[856]: OVS/OF Released Date : 09/10/2024
[61.409729] system-diag[856]: ONIE version : 2021.08-dirty
[61.411365] system-diag[856]: Hardware information:
[61.416826] system-diag[856]: MAC address : 0c:f7:d1:BC:00:00
[61.419458] system-diag[856]: Serial number : 7B4761A76EF6
[61.423470] system-diag[856]: Product name : AS5812_54X
[61.428583] system-diag[856]: PSU:
[61.429789] system-diag[856]: PSU test failed
[61.433571] system-diag[856]: System FAN:
[61.434702] system-diag[856]: Fan 1 Failed, fan speed is 0
[61.439620] system-diag[856]: Fan 2 Failed, fan speed is 0
[61.442462] system-diag[856]: Fan 3 Failed, fan speed is 0
[61.446467] system-diag[856]: Fan 4 Failed, fan speed is 0
[61.451886] system-diag[856]: Fan 5 Failed, fan speed is 0
[61.453788] system-diag[856]: Fan rear 1 Failed, fan speed is 0
[61.460630] system-diag[856]: Fan rear 2 Failed, fan speed is 0
[61.462281] system-diag[856]: Fan rear 3 Failed, fan speed is 0
[61.464576] system-diag[856]: Fan rear 4 Failed, fan speed is 0
[61.470837] system-diag[856]: Fan rear 5 Failed, fan speed is 0
[61.473180] system-diag[856]: Temperature:
[61.475817] system-diag[856]: CPU temperature : 0 C / 32 F
[61.480886] system-diag[856]: Switch chip temperature : 0 C / 32 F
[61.485807] system-diag[856]: Board temperature : N/A

```
[   61.489611] system-diag[856]: Optical modules:
[   61.493579] system-diag[856]:        Optical modules test failed
[   61.495103] system-diag[856]: RTC:
[   61.497815] system-diag[856]:        RTC is OK!
[   61.501146] system-diag[856]:        Time    : 2024-09-11 10:10:36.403331+00:00
[   61.506977] system-diag[856]: Disk space:
[   61.511851] system-diag[856]:        /dev/sda        : 10240 MB
[   61.513867] system-diag[856]:        /dev/sda1       : 2 MB
[   61.517624] system-diag[856]:        /dev/sda2       : 128 MB
[   61.519591] system-diag[856]:        /dev/sda3       : 16 MB
[   61.525635] system-diag[856]:        /dev/sda4       : 2048 MB       (Rootfs)
[   61.527771] system-diag[856]:        /dev/sda5       : 2048 MB
[   61.532598] system-diag[856]:        /dev/sda6       : 5996 MB
[   61.538692] system-diag[856]:        Free space of rootfs partition is 1042 MB.
[   61.540997] system-diag[856]: Memory size:
[   61.545907] system-diag[856]:        Total memory    : 2029724 KB
[   61.547978] system-diag[856]:        Free memory     : 993052 KB
[   61.551585] system-diag[856]: CPU utilization: 51.60%
[   61.556830] system-diag[856]: ************  System Diagnosis End  ************
[  102.771621] nos-init[854]: .

PICOS login:
```

- View the L2/L3 command configurations of client1 and client2.

```
admin@PICOS> configure
Entering configuration mode.
There are no other users in configuration mode.
admin@PICOS# show |display set
    set vlans vlan-id 20
    set vlans vlan-id 30

admin@PICOS#
```

Appendix: ZTP API

The ZTP makes use of the API (application programming interface) defined in the *ztp-functions.sh* file located in the */usr/bin* directory.

The API description is shown as below, and you can refer to it when configuring the ZTP function, such as running the *generate_script* to generate the provision script.

NOTE:

For APIs with name changed, please use the correct name in the corresponding version, or the error prompt will appear.

API	Description	Parameter	Return Value	Supported Version
ztp_disable	Disable ZTP auto-run when switch boots up	None	0 = success, 1 = failed	All
ztp_enable	Enable ZTP auto-run when switch boots up	None	0 = success, 1 = failed	All
add_remote_syslog_server <**ip-addrees**>	Add the remote Syslog server	**Parameter #1**: the IP address of remote Syslog server (eg: 192.168.1.200)	0 = success, 1 = failed	All
remove_remote_syslog_server <**ip-address**>	Remove the remote Syslog server	**Parameter #1**: the IP address of remote Syslog server (eg: 192.168.1.200)	0 = success, 1 = failed	All
tftp_get_file <**file-name1**> <**file-name2**> <**ip-address**>	Get file from TFTP server	**Parameter #1**: file name in TFTP server **Parameter #2**: file name with path in local **Parameter #3**: IP address of TFTP server	0 = success, 1 = failed	All
http_get_file **<file-name> <file-url>**	Get file from HTTP server	**Parameter #1**: file name with path in local **Parameter #2**: file name with HTTP server URL	0 = success, 1 = failed	V4.5.0E or later versions

get_l2l3_config_file <**file-name**> <**ip-address**>	Get PicOS configuration file "pica_startup.boot" from file server	**Parameter #1**: For TFTP download: it is the configuration file name with path on TFTP sever For HTTP download: it is the configuration file name with HTTP server URL. Parameter #2 does not need to be set **Parameter #2**: TFTP server IP address, if not set, the TFTP server IP address from DHCP server will be used	0 = success, 1 = failed	V4.5.0E or later versions **Note**: in the previous versions, the name is tftp_get_l2l3_config_file.
get_ovs_config_file <**file-name**> <**ip-address**>	Get PicOS OVS configuration file "ovs-vswitchd.conf.db" from file server	**Parameter #1**: For TFTP download: it is the configuration file name with path on TFTP sever For HTTP download: it is the configuration file name with HTTP server URL. Parameter #2 does not need to be set **Parameter #2**: TFTP server IP address, if not set, the TFTP server IP address from DHCP server will be used	0 = success, 1 = failed	V4.5.0E or later versions **Note**: in the previous versions, the name is tftp_get_ovs_config_file.
get_picos_startup_file <**file-name**> <**ip-address**>	Get PicOS startup file "picos_start.conf" from file server	**Parameter #1**: For TFTP download: it is the startup file name with path on TFTP sever	0 = success, 1 = failed	V4.5.0E or later versions **Note**: in the previous versions, the name is tftp_get_picos_startup_file.

		For HTTP download: it is the startup file name with HTTP server URL. Parameter #2 does not need to be set **Parameter #2**: TFTP server IP address, if not set, the TFTP server IP address from DHCP server will be used		
get_picos_image <**file-name**> <**ip-address**>	Get PicOS image from file server and upgrade	**Parameter #1**: For TFTP download: it is the image file name with path on TFTP sever For HTTP download: it is the image file name with HTTP server URL. Parameter #2 does not need to be set **Parameter #2**: TFTP server IP address, if not set, the TFTP server IP address from DHCP server will be used	0 = success, 1 = failed	V4.5.0E or later versions **Note**: in the previous versions, the name is tftp_ get_picos_image.
l2l3_load_config <**file-name**> <**ip-address**>	Get a file with PicOS L2/L3 commands list, and execute these commands.	**Parameter #1**: For TFTP download: it is the commands file name with path on TFTP sever For HTTP download: it is the commands file name with HTTP server URL. Parameter #2 does not need to be set	0 = success, 1 = failed	All

		Parameter #2: TFTP server IP address, if not set, the TFTP server IP address from DHCP server will be used		

PICOS Licenses

- License Portal Guide
- Installing License under Linux prompt
- Installing and Removing License for PICOS go2cli Version

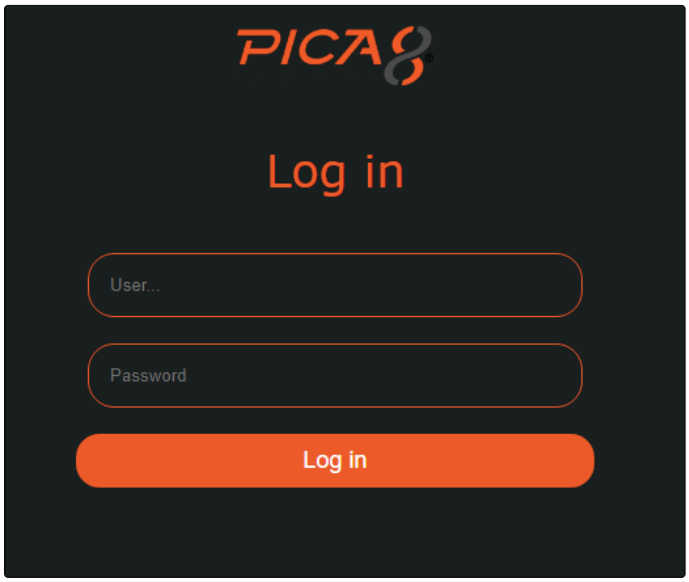
License Portal Guide

Follow the steps below to generate and install the PICOS license.

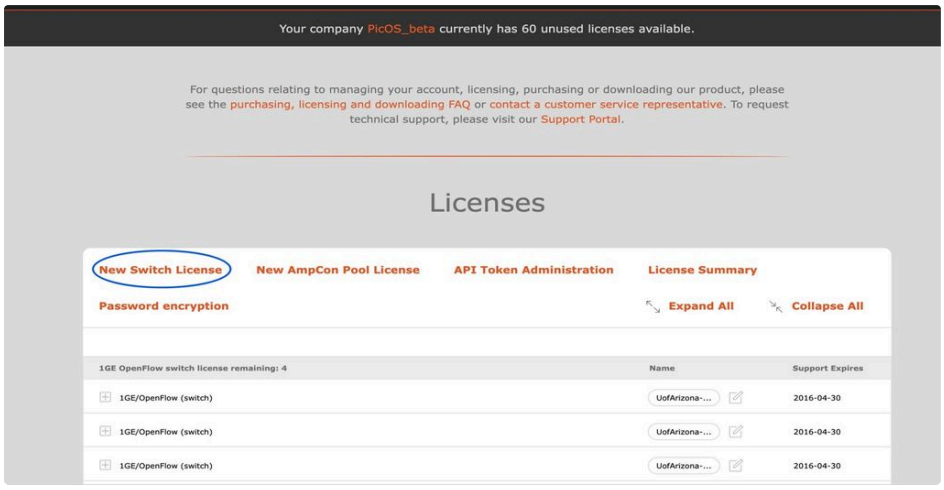
1. Get the switch's speed type and hardware ID by issuing the following command at switch's Linux prompt:

```
admin@XorPlus$ license –s
```

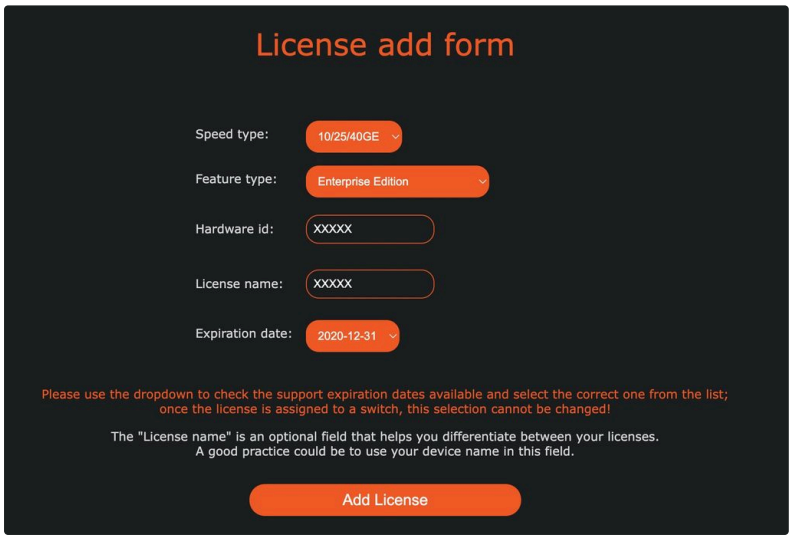
2. Use the assigned credential (SSO) by PICOS License team (*license@pica8.com)* to login at "*License Portal*" website.



3. In the "License Portal" page, click "New Switch License" as shown below:

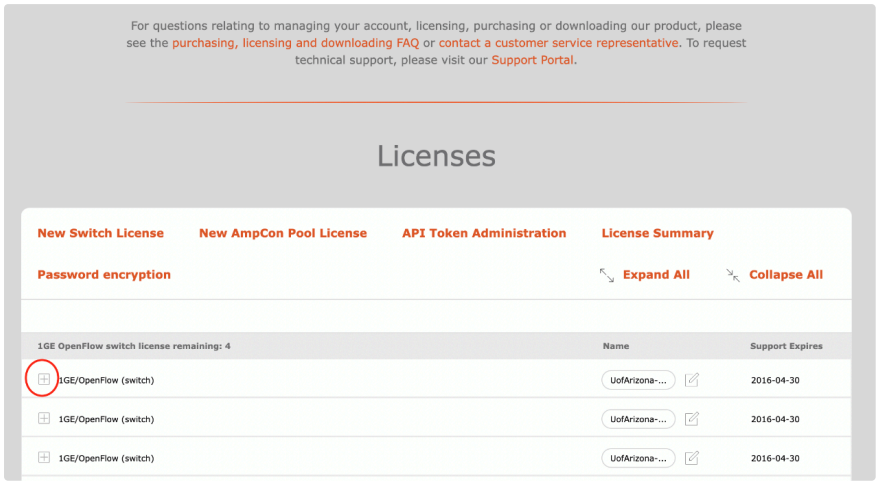


4. In "New Switch License" page, select **Speed type** and **Feature type** based on your purchased order. Then, enter the switch's hardware ID. License name is optional.

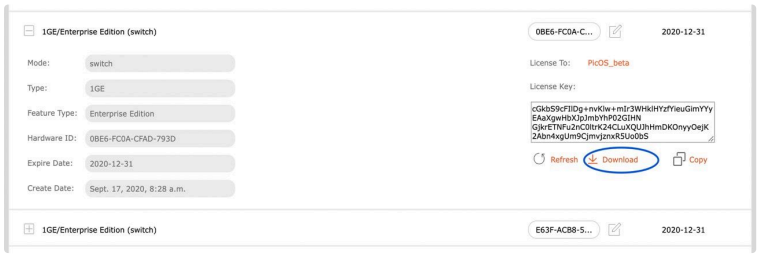


5. After clicking the “Add License” button, the license will be added to the database.

6. Click the “+” sign of the newly added license to display the “Download” button.



7. Click the “Download” button to download the license to the host. The license file name is “hardware_ID.lic”. For example: xxxx-xxxx-xxxx-xxxx.lic



8. Copy the downloaded license file (xxxx.lic) to the switch’s folder /home/admin/ by using scp or tftp etc.

```
admin@XorPlus$ sudo scp xxxx.lic /home/admin/
```

9. Install the license by issuing the following command:

```
admin@XorPlus$ sudo license -i /home/admin/xxxx.lic
```

10. Restart the PICOS service to activate the license:

```
admin@XorPlus$ sudo systemctl restart picos
```

11. After the switch rebooted, use the following command to verify the installed license.

```
admin@XorPlus$ license –s
```

or

```
admin@XorPlus> license show
```

Installing License under Linux prompt

PICOS can be installed on bare metal switches listed in Switch Machine Outline and System Characteristics. A software license is needed to activate PICOS on the specific switch it is installed on.

Please refer to page License Portal Guide, to see how to download licenses for switches.

- Terminology
- PICOS License Types
  - Enterprise License
  - SDN License
- Available Ports without Installing a License
- Speed
- Mode
- Accessing Hardware ID
- Installing the License
- Troubleshooting License Installation
- Displaying License Information
- Removing a License
- License Update on Older Releases
- Add License Directly From License Command

Terminology

The following terms are used throughout this section:

- **Bundle:** This license includes all PICOS features. That is, it *bundles* all three licenses.
- **Evaluation License:** There is *no* evaluation license because users can evaluate PICOS without a license. Please note that only the first four switch ports (and the management port) are active without a license.
- **Hardware ID:** Hardware ID is needed when users download a license. Users can view their own switch ID by executing the license show command **license -s**.
- **Mode:** There are two license modes: switch license and site license.
- **Type:** There are two speed types: 1G and 10G.

PICOS License Types

PICOS includes two types of licenses: Enterprise License and SDN License. Different types of licenses contain different available features. You can purchase the appropriate license according to the network requirements.

Enterprise License

The Enterprise License contains all the features of PICOS, and if you purchase the Enterprise license, all the PICOS features can be applied, which are divided into three types of features: Base Feature, Layer 3 Feature and OpenFlow Feature.

Base Feature

The following features are available as part of the Base feature:

- Network Linux
- Layer 2 (STP/RSTP/MSTP, LLDP, LACP, IGMP-Snooping, dot1x, sFlow, UDLD)

- Multi-chassis Link Aggregation (MLAG)
- Simple Network Management Protocol (SNMP)
- Security
- Zero Touch Provisioning (ZTP)
- Static Routes

Layer 3 Feature

The following features are available as part of the Layer3 feature:

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Protocol-Independent Multicast (PIM)
- Network Address Translation (NAT)
- Virtual Extensible LAN (VXLAN)
- VRRP (Virtual Router Redundancy Protocol)

OpenFlow Feature

The following features are available as part of the OpenFlow feature:

- Open vSwitch Database Management Protocol (OVSDB)
- OpenFlow Releases 1.3 and 1.4
- Multi Protocol Label Switching (MPLS)
- CrossFlow
- Virtual Extensible LAN (VXLAN)

SDN License

The SDN license only includes the OpenFlow feature, and only the OpenFlow feature can be applied with the purchase of an SDN license.

OpenFlow Feature

The following features are available as part of the OpenFlow feature:

- Open vSwitch Database Management Protocol (OVSDB)
- OpenFlow Releases 1.3 and 1.4
- Multi Protocol Label Switching (MPLS)
- CrossFlow
- Virtual Extensible LAN (VXLAN)

Available Ports without Installing a License

If there is no license installed, only the first four ports and the first two uplink ports (if exist) of the switch are available. The first four ports and the first two uplink ports (if exist) should support to enable any protocol whether there is a license or not. This is also the perfect way to test PICOS without buying a full license.

Note that without a license installed, only the first four physical ports and the first two uplink ports (if exist) can be used, not logical ports. If the first two uplink port is split into four interfaces, available ports for Pica8 switches are listed in **Table 1** if no license is installed or the license is expired.

Table 1. Available Ports for Pica8 Switches when no License is Installed

Devices	Available Ports
AS4610 Series Switches	ge-1/1/1, ge-1/1/2, ge-1/1/3, ge-1/1/4

	te-1/1/1,te-1/1/2
AS5712_54X, AS5812_54T, AS5812_54X, S4048-ON, S4128F-ON, S4148F-ON, S4148T-ON	te-1/1/1, te-1/1/2, te-1/1/3, te-1/1/4 xe-1/1/1 (xe-1/1/1.1, xe-1/1/1.2, xe-1/1/1.3, xe-1/1/1.4 after breakout) xe-1/1/2 (xe-1/1/2.1, xe-1/1/2.2, xe-1/1/2.3, xe-1/1/2.4 after breakout)
AS7712_32X, Z9100-ON	xe-1/1/1 (xe-1/1/1.1, xe-1/1/1.2, xe-1/1/1.3, xe-1/1/1.4 after breakout) xe-1/1/2 (xe-1/1/2.1, xe-1/1/2.2, xe-1/1/2.3, xe-1/1/2.4 after breakout) xe-1/1/3 (xe-1/1/3.1, xe-1/1/3.2, xe-1/1/3.3, xe-1/1/3.4 after breakout) xe-1/1/4 (xe-1/1/4.1, xe-1/1/4.2, xe-1/1/4.3, xe-1/1/4.4 after breakout)
AS7816_64X, Z9264F-ON	xe-1/1/1 (xe-1/1/1.1, xe-1/1/1.2, xe-1/1/1.3, xe-1/1/1.4 after breakout) xe-1/1/2 xe-1/1/3 (xe-1/1/3.1, xe-1/1/3.2, xe-1/1/3.3, xe-1/1/3.4 after breakout) xe-1/1/4

Speed

There are two speeds available for each license.

- **1GE:** Platform with 48 x 1GE **OR** 48 x 1GE + 4 x 10GE ports
- **10GE:** Platform with 48 x 10GE + 4 x 40GE **OR** 48 x 10GE + 6 x 40GE **OR** 32 x 40GE ports

Mode

- **Switch:** Use this to install a license on a single switch only.
- **Site:** Use this to install the same license on all switches at a *site*.

Accessing Hardware ID

User must have the hardware ID available to download a license. A utility generates hardware ID using the **license -s** command in PICOS OVS mode.

```
admin@PICOS:/ovs$ license -s
No license installed. Use below information to create a license.
Type: 1GE
```

```
Hardware ID: E385-FB53-4D57-05EB
```

Installing the License

If no license is installed, only the first four ports and the first two uplink ports (if exist) of the switch are available after the upgrade. To upgrade the switch without production impact, user should install a license *before* the upgrade.

It is possible to install a license in PICOS 2.3 (starting with PICOS 2.3.3).

To upgrade a switch from a PICOS version earlier than 2.3, it may be necessary to upgrade to PICOS 2.3 first to install a license on the system. **To avoid this step, user can run a script that can install the license on PICOS releases earlier than 2.3. Please contact Pica8 support or look at the section below for older PICOS releases.**

The license file cannot name pica.lic, or license will install failed.

Customers can download the generated license file and copy it to the */etc/picos/* directory.

The following example shows the contents of a switch-based license file:

```
{
    "Type": "1GE",
    "Feature":["Open Flow", "Base Product", "Layer3"],
    "Hardware ID":"8A68-A7AC-D702-70D2",
    "Expire Date":"2020-10-28"
}
```

In the license file shown above, the type is 1GE while the feature is *Base Product, Layer3,* and *Open Flow*. Hardware ID is unique to every switch.

The switch cannot upgrade to a PICOS version whose build date is later than the license expiration date.

The following example shows the contents of a site-based license file:

```
{
    "Type": "1GE",
    "Feature":["Open Flow", "Base Product", "Layer3"],
    "Mode":"site",
    "Site Name":"CompanyA",
    "Expire Date":"2020-10-28"
}
```

The license file can be installed with the command-line utility called **license** with the **-i** option. The following example installs a license file named *js.lic*:

```
admin@PICOS:~$ cd /etc/picos
admin@PICOS:/etc/picos$ ls -l
total 32
drwxrwxr-x  2 root xorp 4096 Feb  4 22:00 ./
drwxrwxr-x 60 root xorp 4096 Feb  4 21:56 ../
-rw-rw-r--  1 root xorp   26 Feb  4 18:27 fs_status
-rw-r--r--  1 root root  399 Feb  4 21:59 js.lic
-rw-rw-r--  1 root xorp  247 Sep  4  2014 license.conf
-rw-rw-r--  1 root xorp  183 Aug 10  2014 p2files.lst
-rw-rw-r--  1 root xorp  488 Feb  4 18:28 picos_start.conf
-rw-r--r--  1 root root  251 Feb  4 22:00 public.key
admin@PICOS:~$ sudo -i js.lic
License successfully added, the switch need to be rebooted to activate the license.
admin@PICOS:~$ ls -l
```

```
total 32
drwxrwxr-x  2 root xorp 4096 Feb  4 22:00 ./
drwxrwxr-x 60 root xorp 4096 Feb  4 21:56 ../
-rw-rw-r--  1 root xorp   26 Feb  4 18:27 fs_status
-rw-rw-r--  1 root xorp  247 Sep  4  2014 license.conf
-rw-rw-r--  1 root xorp  183 Aug 10  2014 p2files.lst
-rw-r--r--  1 root root  382 Feb  4 22:00 pica.lic
-rw-rw-r--  1 root xorp  488 Feb  4 18:28 picos_start.conf
-rw-r--r--  1 root root  251 Feb  4 22:00 public.key
-rw-r--r--  1 root root  251 Feb  4 22:00 switch-public.key
admin@PICOS:~$
```

If the license is installed successfully, after **license -i** command, the following message will be displayed:

License successfully added, the switch need to be rebooted to activate the license.

To activate the new license, the switch must be restarted.

Troubleshooting License Installation

User may encounter various problems during license installation as detailed below.

- The *public.key* file cannot be found.

```
admin@PICOS:~$ sudo license -i js.lic
Install failed: Cannot find public key.
```

- The license file does not exist.

```
admin@PICOS:~$ sudo license -i js.lic
Install failed: No such file or directory.
```

- The header or the key is disrupted.

```
admin@PICOS:~$ sudo license -i js.lic
Install failed: License or KEY is disrupted.
```

- The license format is not valid.

```
admin@PICOS:~$ sudo license -i js.lic
Install failed: License format error.
```

- The license file is not compatible with the switch (verify failed).

```
admin@PICOS:~$ sudo license -i js.lic
Install failed: Invalid license.
```

Displaying License Information

User can display the license information using the **license -s** command at the Linux shell.

The following example displays information about the switch-based license:

```
admin@PICOS:~$ license -s
{
        "Type": "1GE",
        "Feature":      ["Open Flow", "Base Product", "Layer3"],
        "Expire Date":  "2020-10-28",
        "Hardware ID":  "8A68-A7AC-D702-70D2"
```

```
}
```

The following example displays information about the site-based license:

```
admin@PICOS:~$ license -s
{
          "Type": "1GE",
          "Feature":      ["Base Product", "Layer3", "Open Flow"],
          "Expire Date":  "2020-10-28",
          "Hardware ID":  "8A68-A7AC-D702-70D2",
          "Site Name":    " CompanyA "
}
```

If the license is not valid, the **license -s** command generates the following output:

```
admin@PICOS:~$ license -s
Invalid license. Use below information to create a license.
Type: 1GE
Hardware ID: 8A68-A7AC-D702-70D2
admin@PicOS-OVS$
```

If no license is installed, the **license -s** command generates the following output:

```
admin@PICOS:~$ license -s
No license installed. Use below information to create a license.
Type: 1GE
Hardware ID: 8A68-A7AC-D702-70D2
admin@PicOS-OVS$
```

Removing a License

User can use the **license -r** command at the Linux shell to remove a license as detailed below:

```
admin@PICOS:~$ cd /etc/picos
admin@PICOS:/etc/picos$ ls -l
total 32
drwxrwxr-x  2 root xorp 4096 Feb  4 22:00 ./
drwxrwxr-x 60 root xorp 4096 Feb  4 21:56 ../
-rw-rw-r--  1 root xorp   26 Feb  4 18:27 fs_status
-rw-rw-r--  1 root xorp  247 Sep  4  2014 license.conf
-rw-rw-r--  1 root xorp  183 Aug 10  2014 p2files.lst
-rw-r--r--  1 root root  382 Feb  4 22:00 pica.lic
-rw-rw-r--  1 root xorp  488 Feb  4 18:28 picos_start.conf
-rw-r--r--  1 root root  251 Feb  4 22:00 public.key
-rw-r--r--  1 root root  251 Feb  4 22:00 switch-public.key
admin@PICOS:$ pwd
/etc/picos
admin@PICOS:~$
admin@PICOS:~$ license -r
admin@PICOS:~$ ls -l
total 28
drwxrwxr-x  2 root xorp 4096 Feb  4 22:05 ./
drwxrwxr-x 60 root xorp 4096 Feb  4 21:56 ../
-rw-rw-r--  1 root xorp   26 Feb  4 18:27 fs_status
-rw-rw-r--  1 root xorp  247 Sep  4  2014 license.conf
-rw-rw-r--  1 root xorp  183 Aug 10  2014 p2files.lst
-rw-rw-r--  1 root xorp  488 Feb  4 18:28 picos_start.conf
-rw-r--r--  1 root root  251 Feb  4 22:00 public.key
```

```
-rw-r--r--  1 root root  251 Feb  4 22:00 switch-public.key
admin@XorPlus$
```

If the license is modified or removed, the switch must be rebooted for the change to be effective.

License Update on Older Releases

To upgrade a switch to PICOS 2.4 from a version earlier than 2.3, it may be necessary to upgrade to PICOS 2.3 first and install a license on the system. To avoid this extra step, user can install a new script on PICOS releases prior to 2.3 and use the script to install a license.

This new script supports the PICOS releases 2.1, 2.2, and 2.3. User has to follow the following steps to install a license using the script:

1. Download the file named *license-powerpc.bin* or *license-powerpcspe.bin* according to the switch model. For example, download the file *license-powerpc.bin* for the Pica8 P-3290 switch.
2. Run the command **./license-powerpc -s** to display the hardware ID.
3. Copy the *upgrade.sh* script from https://github.com/Pica8/Upgrade to the switch.
4. Copy the license tool from http://www.pica8.com/portal/standard/ to the switch. The tool can be used to install a license on PICOS 2.3 or earlier but the license will only become effective after upgrading to PICOS 2.4 or later.

The Pica8 P-3290 and P-3295 use the *license-powerpc* file. All other PICOS switches use the *license-powerpcspe* file.

The following example describes how to upgrade a Pica8 P-3297 switch from PICOS 2.3.

Step 1: Check the version of PICOS using the **version** command at the Linux shell.

```
admin@PICOS:~$ version
Copyright (C) 2009-2024 Pica8, Inc.
==================================
Base ethernet MAC Address     : 28:e4:24:4c:42:ef
Hardware Model                : N9550-64D
Linux System Version/Revision : 4.4.6-rc1/19ef739fab
Linux System Released Date    : 10/15/2024
L2/L3 Version/Revision        : 4.4.6-rc1/19ef739fab
L2/L3 Released Date           : 10/15/2024
OVS/OF Version/Revision       : 4.4.6-rc1/19ef739fab
OVS/OF Released Date          : 10/15/2024
```

Step 2: Copy license tool:

```
admin@PICOS:~$ cd /etc/picos
admin@PICOS:~$ ls -l
total 20
drwxrwxr-x  2 root xorp 4096 Jun 29 08:01 ./
drwxrwxr-x 60 root xorp 4096 Jun 29 08:03 ../
-rw-rw-r--  1 root xorp   26 Jun 29 08:01 fs_status
-rw-rw-r--  1 root xorp  183 Jun 30  2014 p2files.lst
-rw-rw-r--  1 root xorp  488 Jun 29 08:01 picos_start.conf
admin@PICOS:~$
```

Step 3: Copy public.key, license.conf and license to /etc/picos:

```
admin@PICOS:~$ ls -l
total 132
drwxrwxr-x  2 root xorp  4096 Jun 29 08:09 ./
drwxrwxr-x 60 root xorp  4096 Jun 29 08:03 ../
-rw-r--r--  1 root root   354 Jun 29 08:09 1GE-SITE-PICA8.lic
```

```
-rw-rw-r--  1 root xorp    26 Jun 29 08:01 fs_status
-rwxr-xr-x  1 root root 98575 Jun 29 08:08 license-powerpc*
-rw-rw-r--  1 root xorp   183 Jun 30  2014 p2files.lst
-rw-rw-r--  1 root xorp   548 Jun 29 08:07 picos_start.conf
-rw-r--r--  1 root root   251 Jun 29 08:07 public.key
admin@PICOS:~$ ./license-powerpc -s
No license installed. Use below information to create a license.
Type: 1GE
Hardware ID: A326-8F2D-3661-AE76
```

Step 4: Install license:

```
admin@PICOS:/ovs$ sudo ./license-powerpcspe -i 1GE-SITE-PICA8.lic
License successfully added, the switch need to be rebooted to activate the license.
admin@PICOS:/ovs$
```

Add License Directly From License Command

User can also add the license directly from the license command. The PICOS 2.6 image supports this command.

Step 1: Paste the license content.

Step 2: Press enter and then press crtl+d.

Example for P5401, add a site license:

```
admin@PICOS:/ovs$ sudo license -i -
sJXhrpDdd2ZsMemcJ26fqvjjw7vH30gf/4OVtLsROgPNl2VjFQhIJvS3zliF+DK+
tW2QpssH0JB4n8ae9/SumsRWdwdPpbQNB1WaeNq0onWdoTRz2HGiH+XudDAm6B37
kQvCGev7pAe0tCjnB+63F3Z5ZGPbQE89/fNSBGkE6mfZ6dG1F/86C9Bn/MyqkQSI
4uDtRwfo46elZOmwn5aD/mGyh/i2qg8IfhssIn0CbHVaJY8hyt7tYuvgkEb6Xlhx
7i9+qnk9c15ksBdak0f8gxorZDOCacwWACDt/K8NJokOMWTDLnLmDczrXO0Z5l75
eGc7ZygxCjd/jzc5oW9cgIyd
License successfully added, the switch need to be rebooted to activate the license.
admin@PICOS:/ovs$
```

Reboot system and license can be activated.

Installing and Removing License for PICOS go2cli Version

- Installing License under CLI Operation Mode
- Removing License under CLI Operation Mode

Installing License under CLI Operation Mode

The following steps describe how to install a license under CLI operation mode for PICOS go2cli version.

Step 1 Before loading a license, upload the license file to the device. The following example uploads the license file **10GE-SITE-PICA8.lic** to the default path.

By default, the TFTP downloaded file is saved in directory **/cftmp/**.

```
admin@PICOS> file tftp get remote-file /tftp/license/10GE-SITE-PICA8.lic local-file 10GE-SITE-PICA8.lic ip-address 10.10.50.22
```

Step 2 Run the **license install** <*file-name*> command to install the license.

```
admin@PICOS> license install /cftmp/10GE-SITE-PICA8.lic
```

When the license has been successfully installed, it will display the following information:

```
License successfully added, the switch need to be rebooted to activate the license.
```

Step 3 Reboot the switch or restart PICOS to activate the license. Choose either one:

- Reboot the switch

```
admin@PICOS> request system reboot
```

- Restart PICOS service

```
licadmin@PICOS> start shell sh
admin@PICOS:~$ sudo service picos restart
admin@PICOS:~$ exit
exit

admin@PICOS>
```

Step 4 After PICOS starts up, run the **license show** command to view the license information.

```
admin@PICOS> license show
{
               "Type":    "10GE",
               "Feature": ["Base Product", "Layer3", "OpenFlow"],
               "Support End Date":  "2020-10-28",
               "Hardware ID":        "196B-A2AE-147A-73F2",
               "Site Name":            "PICA8"
}
```

Removing License under CLI Operation Mode

The following steps describe how to remove a license under CLI operation mode for PICOS go2cli version.

```
admin@PICOS> license remove
admin@PICOS> license show
No license installed. Use below information to create a license.
Type: 10GE
Hardware ID: 196B-A2AE-147A-73F2
```

PICOS Mode Selection

PicOS can run in two different modes:

- L2/L3 Mode
- OVS Mode

L2/L3 Mode

In the L2/L3 (Layer 2 / Layer 3) mode, PicOS can run switching and routing protocols, as well as OpenFlow applications. In this mode, L2/L3 daemons are running, but OVS can also be activated if OpenFlow in Crossflow Mode is enabled.

OVS Mode

In the OVS (Open vSwitch) mode, PicOS is optimized for OpenFlow applications. In this mode, L2/L3 daemons are not running, and the system is fully dedicated to OpenFlow and OVS.

Helpful related pages:

- Changing PicOS Mode by Modifying the Boot File
- PicOS Boot File
- Changing PicOS Mode from CLI

Changing PicOS Mode by Modifying the Boot File

The PicOS boot configuration is kept in the **picos_start.conf** file located at */etc/picos.*

```
admin@LEAF-A$ls /etc/picos/picos_start.conf
/etc/picos/picos_start.conf
```

User can use the **cat** command at the Linux shell to display the contents of the **picos_start.conf** file.

```
admin@LEAF-A$cat /etc/picos/picos_start.conf
[PICOS]
picos_start=xorplus

[XORPLUS]
xorplus_rtrmgr_verbose=
xorplus_log_facility=local0
xorplus_finder_client_address=127.0.0.1
xorplus_finder_server_address=127.0.0.1

[OVS]
ovs_database_file=/ovs/ovs-vswitchd.conf.db
ovs_inband_database_file=/ovs/inband.conf.db
ovs_inventory_database_file=/tmp/inventory.conf.db
inventory_schema=/ovs/share/openvswitch/inventory.ovsschema
ovs_function_database_file=/ovs/function.conf.db
function_schema=/ovs/share/openvswitch/function.ovsschema
ovs_portGroup_database_file=/ovs/portGroup.conf.db
portGroup_schema=/ovs/share/openvswitch/portGroup.ovsschema
ovs_db_sock_file=/ovs/var/run/openvswitch/db.sock
ovs_invd_file=/ovs/share/openvswitch/scripts/ovs-invd
ovs_invd_python_path=/ovs/share/openvswitch/python
ovs_db_manager=Open_vSwitch,Manager,target
ovs_switch_ip_address=10.10.51.199
ovs_switch_ip_netmask=255.255.255.0
ovs_switch_gateway_ip=10.10.51.1
ovs_switch_tcp_port=6640
ovs_host_name=PICOS-OVS
ovs_use_dhcp=false
ovs_enable_lighttpd=false
ovs_enable_snmpd=false
ovs_enable_npb=false
ovs_enable_mgp_ipv6=false
ovs_output_syslog_local=true

[ZTP]
ztp_disable=false
otp_disable=true
```

The **picos_start** option in the **[PICOS]** section of the **picos_start.conf** file dictates the PicOS mode (L2/L3 or OVS). The **picos_start** option has two possible values: **xorpplus** and **ovs**.

To change the PicOS mode, user has to open the **picos_start.conf** file in a text editor like **vi** and change the value of **picos_start**. After changing the value and saving the file, user must restart the **picos** service to bring the PicOS mode change into effect.

The following example shows an excerpt from the **picos_start.conf** file. If the value of **picos_start** is **ovs**, PicOS will run in OVS mode after the next **PicOS** restart.

```
picos_start=ovs
```

Once the **picos_start.conf** file has been updated, user needs to restart the **picos** service by using the **sudo systemctl restart picos** command, or rebooting the switch.

```
admin@LEAF-A$sudo systemctl restart picos
(No print here, it will cost few minutes for PICOS to restart.)
admin@LEAF-A$
```

User is in PicOS OVS mode now.

The following example shows an excerpt from the **picos_start.conf** file. If value of **picos_start** is **xorpplus,** PicOS will run in L2/L3 mode after the next **PicOS** restart.

```
picos_start=xorplus
```

Once the **picos_start.conf** file has been updated, user needs to restart the **picos** service by using the **sudo systemctl restart picos** command or by rebooting the switch.

```
admin@LEAF-A$sudo systemctl restart picos
(No print here, it will cost few minutes for PICOS to restart.)
admin@LEAF-A$
```

Once the switch is in L2/L3 mode, user can use the **cli** command at the Linux shell to reach the L2/L3 operation mode.

```
admin@LEAF-A$cli
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on LEAF-A
admin@LEAF-A>
```

PicOS Boot File

The Pica8 PICOS software keeps its boot configuration in the **picos_start.conf** file located in the **/etc/picos** directory.

```
admin@LEAF-A$ ls /etc/picos/picos*
/etc/picos/picos_start.conf
```

User can use the **more** command at the Linux shell to display contents of the **picos_start.conf** file.

```
admin@LEAF-A$ more /etc/picos/picos_start.conf
[PICOS]
picos_start=xorplus

[XORPLUS]
xorplus_rtrmgr_verbose=
xorplus_log_facility=local0
xorplus_finder_client_address=127.0.0.1
xorplus_finder_server_address=127.0.0.1

[OVS]
ovs_database_file=/ovs/ovs-vswitchd.conf.db
ovs_inband_database_file=/ovs/inband.conf.db
ovs_inventory_database_file=/tmp/inventory.conf.db
inventory_schema=/ovs/share/openvswitch/inventory.ovsschema
ovs_function_database_file=/ovs/function.conf.db
function_schema=/ovs/share/openvswitch/function.ovsschema
ovs_portGroup_database_file=/ovs/portGroup.conf.db
portGroup_schema=/ovs/share/openvswitch/portGroup.ovsschema
ovs_db_sock_file=/ovs/var/run/openvswitch/db.sock
ovs_invd_file=/ovs/share/openvswitch/scripts/ovs-invd
ovs_invd_python_path=/ovs/share/openvswitch/python
ovs_db_manager=Open_vSwitch,Manager,target
ovs_switch_ip_address=10.10.51.199
ovs_switch_ip_netmask=255.255.255.0
ovs_switch_gateway_ip=10.10.51.1
ovs_switch_tcp_port=6640
ovs_host_name=PICOS-OVS
ovs_use_dhcp=false
ovs_enable_lighttpd=false
ovs_enable_snmpd=false
ovs_enable_npb=false
ovs_enable_mgp_ipv6=false
ovs_output_syslog_local=true

[ZTP]
ztp_disable=false
otp_disable=true
```

The **picos_start.conf** boot file has the following four sections, each section having one or more variables:

1. PICOS
2. XORPLUS
3. OVS
4. ZTP

The following table describes the variables in **picos_start.conf** - the PicOS boot file.

Section	Variable	Value	Description
PICOS	**picos_start**	**xorplus**	PICOS operates in the L2/L3 mode after the **picos** service is restarted, or the system is rebooted.
		ovs	PICOS operates in the OVS mode after the **picos** service is restarted, or the system is rebooted.
			The device boots into Linux as usual, but both the PICOS modes are *inactive*.
XORPLUS	**xorplus_rtrmgr_verbose**		Indicates that the xorplus_rtrmgr log is in use.
	xorplus_log_facility		Configures the logging facility.
	xorplus_finder_client_address		Configures IP address.
	xorplus_finder_server_address		Configures IP address.
OVS	**ovs_database_file**		Defines the Open vSwitch configuration database.
	ovs_inband_database_file		Defines the Open vSwitch inband configuration database.
	ovs_db_sock_file		Defines the Unix domain socket file for communication between **ovsdb-server** and **ovs-vswitchd**.
	ovs_switch_ip_address		Defines the Open vSwitch management IP address.
	ovs_switch_ip_netmask		Defines the subnet mask for the Open vSwitch management IP address.
	ovs_switch_gateway_ip		Defines the gateway for the Open vSwitch management IP address.
	ovs_switch_tcp_port		Defines the TCP port for communication between **ovsdb_server** and **ovs-vswitchd**.
	ovs_host_name		Defines the Open vSwitch host name.
	ovs_use_dhcp	**true**	Indicates that the Open vSwitch is getting its management IP address through DHCP.
		false	Indicates that the Open vSwitch is configured with a static management IP address.
ZTP	**ztp_disable**	**true**	Indicates that ZTP (Zero Touch Provisioning) is disabled.
		false	Indicates that ZTP (Zero Touch Provisioning) is enabled.
	otp_disable	**true**	Indicates that the OTP function is disabled.
		false	Indicates that the OTP function is enabled.

Changing PicOS Mode from CLI

User can switch between L2/L3 and OVS modes using the **picos_boot** script already included in PicOS. User can run the script from the Linux shell on user's PicOS switch. The script will modify the PicOS boot file */etc/picos/picos_start.conf* automatically, without user having to edit the file manually.

Warning:

On FS S5810 Series and S5860 Series switches, run "save_config" command when perform picos_boot. Otherwise, the picos_boot configuration will be lost after PicOS reboot. For detail, please refer to Configuration Saving Guide.

Switching from L2/L3 Mode to OVS Mode

This section describes the procedure to switch from the L2/L3 mode to OVS mode on a PicOS switch named **LEAF-A**. The switch name is arbitrary.

1. Login with username **admin** to arrive at the Linux shell prompt.

```
Username: admin
Password:
admin@LEAF-A$
```

NOTE:

For PICOS **go2cli** version, users go to PICOS CLI prompt after log in:

```
admin@Xorplus>
```

At PICOS CLI prompt, run "**start shell sh**" to enter Linux shell.

```
admin@Xorplus> start shell sh
admin@Xorplus:~$
```

2. Run the **picos_boot** script located in */usr/bin* directory. The full path does not need to be used because the /usr/bin directory is on the system **PATH** by default.

3. Enter option **2** to select OVS mode.

4. Choose how the IP address of the management interface should be configured: DHCP or static IP. If *Static IP* is chosen, values for static IP address, subnet mask, and default gateway must be provided. If *DHCP* is chosen, no more questions are asked.

```
admin@PICOS:~$ sudo picos_boot
Configure default startup options:
(Select key 3 if no change)
[1] PICOS L2/L3
[2] PICOS Open vSwitch/OpenFlow * default
```

```
[3] Quit
Enter your choice (1,2,3):2

PICOS Open vSwitch/OpenFlow is selected.

Configure management interface(IPv4):
[1] DHCP * default
[2] Static
Enter your choice(1,2):
```

5. Restart the **picos** service to activate PicOS OVS mode.

```
admin@LEAF-A$ exit
admin@LEAF-A> request system reboot
(No print here, it will cost few minutes for PICOS to restart.)
admin@LEAF-A$
```

As an alternative to restarting the **picos** service, user can just reboot the switch to bring the PicOS mode change into effect.

```
admin@LEAF-A$sudo reboot
Broadcast message from root@PicOS-OVS (pts/0) (Sun Aug 16 21:18:48 2015):
The system is going down for reboot NOW!

Username: admin
Password:
admin@PicOS-OVS$
```

The **picos_boot** script has the following options:

Option 1 selects the PICOS L2/L3 (Layer 2 / Layer 3) mode. When user chooses option 1, PICOS will load in L2/L3 mode after a reboot.

Option 2 selects the PICOS OVS (Open vSwitch) mode. When user chooses option 2, PICOS will load in OVS mode after a reboot.

Option 3 does not modify the present PICOS mode.

Switching from OVS Mode to L2/L3 Mode

This section describes the procedure used to switch from OVS mode to L2/L3 mode on a PicOS switch named **LEAF-A**. The switch name is arbitrary.

1. Log in with username **admin** to arrive at the Linux shell prompt.

```
Username: admin
Password:
admin@PicOS-OVS$
```

NOTE:

For PICOS **go2cli** version, users go to PICOS CLI prompt after log in:

```
admin@Xorplus>
```

At PICOS CLI prompt, run "**start shell sh**" to enter Linux shell.

```
admin@Xorplus> start shell sh
admin@Xorplus:~$
```

2. Run the **picos_boot** script located in */usr/bin* directory. The full path does not need to be used because the /usr/bin directory is on the system **PATH** by default.

3. Enter option **1** to select L2/L3 mode.

```
admin@PicOS-OVS$sudo picos_boot
Configure the default system start-up options:
 (Select key 3 if no change)
    [1]  PICOS L2/L3
    [2]  PICOS Open vSwitch/OpenFlow   * default
    [3]  No start-up change
Enter your choice (1,2,3):1
PICOS L2/L3 switch system is selected.
Please restart the PICOS service
```

4. Restart the **picos** service to activate PicOS L2/L3 mode.

```
admin@PicOS-OVS$ exit
admin@PicOS-OVS> request system reboot
(No print here, it will cost few minutes for PICOS to restart.)
admin@PicOS-OVS$
```

5. Optionally, user can run the **cli** command at the Linux shell to enter the PicOS L2/L3 operation mode.

```
admin@PicOS-OVS$cli
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on LEAF-A
admin@LEAF-A>
```

As an alternative to restarting the **picos** service, user can just reboot the switch to bring the PicOS mode change into effect.

Enabling CrossFlow in L2/L3 Mode

This section describes the procedure to enable CrossFlow in L2/L3 mode.

1. Enter L2/L3 operation mode, using the **cli** command at the Linux shell.

```
admin@LEAF-A$ cli
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on LEAF-A
admin@LEAF-A>
```

NOTE:

This step is not necessary for PICOS **go2cli** version, as users go to PICOS CLI prompt after log in:

```
admin@Xorplus>
```

At PICOS CLI prompt, run “**start shell sh**” to enter Linux shell.

```
admin@Xorplus> start shell sh
admin@Xorplus:~$
```

If you want to return from the Linux shell back to the CLI prompt, run "**exit**".

```
admin@Xorplus:~$ exit
exit

admin@Xorplus>
```

2. Enter configuration mode, using the **configure** command in the operation mode.

```
admin@LEAF-A> configure
Entering configuration mode.
There are no other users in configuration mode.
admin@LEAF-A#
```

3. Enable CrossFlow mode, using the **set xovs enable true** command in configuration mode. Commit the changes, and exit the configuration mode. Then, exit the operation mode.

```
admin@LEAF-A# set xovs enable true
admin@LEAF-A# commit
Commit OK.
Save done.
admin@LEAF-A# exit
admin@LEAF-A> exit
admin@LEAF-A$
```

4. User can now run the OVS mode commands from the Linux shell.

```
admin@LEAF-A$ovs-vsctl show
e8e63632-d96b-409a-89c3-95bb4ef61f46
    Bridge "ECODE3"
        Controller "tcp:65.19.141.118:6633"
            is_connected: true
        Port "ge-1/1/1"
            Interface "ge-1/1/1"
                type: "pica8"
        Port "ECODE3"
            Interface "ECODE3"
```

```
                type: internal
        Port "ge-1/1/47"
            Interface "ge-1/1/47"
                type: "pica8"
        Port "ge-1/1/48"
            Interface "ge-1/1/48"
                type: "pica8"
        Port "ge-1/1/2"
            Interface "ge-1/1/2"
                type: "pica8"
```

PICOS Password Recovery

This document is used to recover a forgotten password. It operates only on the console port, and it depends on the platforms.

- Password Recovery for X86 Platform
- Password Recovery for AS4610 Series Switches
- Password Recovery Guide for FS S5810/S5860 Series Switches
- Password Recovery Guide for FS N8560-32C

Password Recovery for X86 Platform

This guide provides the procedure for recovering the **admin** account password login from the ETH interface for X86 platform switches. If you forget the admin password, use the password recovery procedure to reset the admin password.

Step1 Login to the switch through the console port.

Step2 Power cycle the switch.

Step3 Enter ONIE.

```
+----------------------------------------------------------------------------+
| PicOS                                                                      |
|*ONIE                                                                       |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
     Use the ^ and v keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Step4 From GRUB prompt, Choose **ONIE: Rescue** to boot ONIE in rescue mode.

```
                  GNU GRUB  version 2.02~beta2+e4a1fe391
+----------------------------------------------------------------------------+
| ONIE: Install OS                                                           |
|*ONIE: Rescue                                                               |
| ONIE: Uninstall OS                                                         |
| ONIE: Update ONIE                                                          |
| ONIE: Embed ONIE                                                           |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
+----------------------------------------------------------------------------+
```

Step5 Check out the partition on which "PICOS-GRUB" resides.

```
ONIE:/ # blkid
/dev/sda6: LABEL="User-Data" UUID="da55e09c-0e7b-4d96-a8c9-bee2ed5bb42c"
/dev/sda5: LABEL="PicOS2" UUID="3f228548-64c1-492c-ad3d-8ca7d248c11a"
/dev/sda4: LABEL="PicOS" UUID="039453f9-0879-4c86-9e0b-8ef4d34d9a66"
/dev/sda3: LABEL="PICOS-GRUB" UUID="b3a8ab95-43f9-4f21-9c76-7f48101be381"
/dev/sda2: LABEL="ONIE-BOOT" UUID="7fcaa6c8-d174-42c1-abd1-8c6eea46eb6b"
/dev/sda1: LABEL="EFI System" UUID="36E9-D2F5"
ONIE:/ #
```

We find that the partition of **LABEL="PICOS-GRUB"** is **/dev/sda3**.

Step6 Issue the following commands to check whether the currently running system is PicOS or PicOS2 in the partition running "PICOS-GRUB".

In this example, "PICOS-GRUB" is on partition **/dev/sda3** according to *Step 5*, so we mount **/dev/sda3**.

```
# mount /dev/sda3 /mnt
ONIE:/ # cat /mnt/grub/grubenv
# GRUB Environment Block
```

```
##############################################################################################################################
default=PICOS-3.8.0.1+1
##############################################################################################################################
ONIE:/ #

ONIE:/ # cat /mnt/grub/grub.cfg
serial --port=0x3f8 --speed=115200 --word=8 --parity=no --stop=1
terminal_input serial
terminal_output serial

set timeout=5
if [ -s $prefix/grubenv ]; then
  load_env
fi
if [ "${next_entry}" ] ; then
   set default="${next_entry}"
   set next_entry=
   save_env next_entry
fi

if [ "${saved_entry}" ] ; then
   set default="${saved_entry}"
   set saved_entry=
   save_env saved_entry
fi

 menuentry PICOS-3.8.0.1+2 {
        search --no-floppy --label --set=root PicOS
        linux /boot/vmlinuz root=LABEL=PicOS rw fsck.mode=force fsckfix  rootfstype=ext4 console=ttyS0,115200n8 int
        initrd /boot/initrd.img
}

menuentry PICOS-3.8.0.1+1 {
        search --no-floppy --label --set=root PicOS2
        linux /boot/vmlinuz root=LABEL=PicOS2 rw fsck.mode=force fsckfix  rootfstype=ext4 console=ttyS0,115200n8 in
        initrd /boot/initrd.img
}

menuentry ONIE {
        search --no-floppy --label --set=root "EFI System"
        echo    'Loading ONIE ...'
        chainloader /EFI/onie/grubx64.efi
}
ONIE:/ #
```

1) First, find out the default version of the system.

From the line with "default=PICOS-3.8.0.1+1", we find that the default version of the system is **PICOS-3.8.0.1**, and the label is 1.

2) Then, check out whether the currently running system is PicOS or PicOS2.

According to "PICOS-3.8.0.1+1", find the following block. In this block, there is "label --set=root PicOS2", it means the running system is **PicOS2**.

```
menuentry PICOS-3.8.0.1+1 {
        search --no-floppy --label --set=root PicOS2
        linux /boot/vmlinuz root=LABEL=PicOS2 rw fsck.mode=force fsckfix  rootfstype=ext4 console=ttyS0,115200n8 in
        initrd /boot/initrd.img
}
```

Step7 From the ONIE prompt, perform the following commands to mount the current boot partition.

```
ONIE:/ # blkid
/dev/sda6: LABEL="User-Data" UUID="da55e09c-0e7b-4d96-a8c9-bee2ed5bb42c"
/dev/sda5: LABEL="PicOS2" UUID="3f228548-64c1-492c-ad3d-8ca7d248c11a"
/dev/sda4: LABEL="PicOS" UUID="039453f9-0879-4c86-9e0b-8ef4d34d9a66"
/dev/sda3: LABEL="PICOS-GRUB" UUID="b3a8ab95-43f9-4f21-9c76-7f48101be381"
/dev/sda2: LABEL="ONIE-BOOT" UUID="7fcaa6c8-d174-42c1-abd1-8c6eea46eb6b"
/dev/sda1: LABEL="EFI System" UUID="36E9-D2F5"
/dev/mmcblk0p2: LABEL="EDA-DIAG" UUID="48f14bec-740e-4aa2-9605-f32de15f9f2c"
/dev/mmcblk0p1: LABEL="EFI System" UUID="3D0E-3759"
```

```
ONIE:/ # mount /dev/sda5 /mnt/              // The partition is based on the step 6.
```

Step8 Modify the shadow file.

```
# vi etc/shadow
```

Change the following line from:
admin:**1eE9WFgVk$EwGcNl83uK98.r8TcKn2q/**:15385:0:99999:7:::
into:
admin::15385:0:99999:7::: //Remove the string between the first and the second colon

Step9 Execute the sync operation.

```
# sync
```

The subsequent steps are distinguished between devices currently running in OVS and L2/L3 mode. Please choose the appropriate steps according to the PicOS mode.

Note: You can refer to the document Checking PicOS Mode to check the current PicOS mode of the device.

- If the running PicOS mode is L2/L3 mode, go to L2/L3 Mode.
- If the running PicOS mode is OVS mode, go to OVS Mode.

L2/L3 Mode:

Step10 Modify the configuration file.

```
ONIE:/# vi pica/config/pica_startup.boot
```

In the pica_startup.boot file, you will find lines starting with "***user admin {***", remove lines of user admin configurations.

For example, remove the following six lines in configuration file.

```
user admin {
            authentication {
                plain-text-password: "$1$zL8TUrpq$/Y1tcx1IhwPkm6HEd4aEM/"
            }
            class: "super-user"
        }
```

Save and exit with ":wq".

Copy the configuration file to the backup file.

```
ONIE:/# cp /mnt/pica/config/pica_startup.boot /mnt/backup/pica/config/pica_startup.boot
ONIE:/# sync
```

Step11 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step12 When you see PicOS login again, you can log in by the admin user without a password.

Step13 Set a new admin password using the following CLI commands and save the configuration.

```
root@XorPlus# set system login user admin authentication plain-text-password pica8           //Please enter the ne
root@XorPlus# set system login user admin class "super-user"
root@XorPlus# commit
```

After the above steps, you can log into the system with the new password.

OVS Mode：

Step10 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step11 Set a new admin password with **passwd admin** command and save the configuration. The commands are illustrated here:

```
root@XorPlus:~$ passwd admin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

After the above steps, you can log into the system with the new password.

Password Recovery for AS4610 Series Switches

This guide provides the procedure for recovering the **admin** account password login from the ETH interface for AS4610 series switches. If you forget the admin password, use the password recovery procedure to reset the admin password.

Step1 Login to the switch through the console port.

Step2 Power cycle the switch.

Step3 Enter uboot prompt. Please hit any key when see the message "Hit any key to stop autoboot:" on console display.

```
....
Hit any key to stop autoboot:  0
accton_as4610-54->
```

Step4 Issue "**run onie_rescue**" to enter ONIE recue mode.

```
accton_as4610-54-> run onie_rescue
```

Step5 Enter ONIE prompt. Please hit any key when see the following message on console display.

```
...

Please press Enter to activate this console. etc_watchdog can't access PHY, forcing link up
...
ONIE:/ #
```

Step6 Issue command "**blkid**" to see which partitions (where LABEL="**PicOS2**" and LABEL="**PicOS**") are used by PicOS. If your outputs are different from what show below, please forward us the outputs.

```
ONIE:/ # blkid
/dev/sda4: LABEL="User-Data" UUID="14574a7e-34fb-450c-be05-690a71e023d9"
/dev/sda1: LABEL="ACCTON-DIAG" UUID="aa56682f-b0f1-4087-8722-42b16a5703ab"
/dev/sda3: LABEL="PicOS2" UUID="3d744634-4c03-4d53-9d04-33205f0606a8"
/dev/sda2: LABEL="PicOS" UUID="afffc6ab-2983-4452-9e90-7a653fef9a90"
```

Step7 According to the above outputs, there are two partitions (**/dev/sda2** and **/dev/sda3**) installed PicOS. Here, we modify shadow file on both partitions.

a) Mount */dev/sda2*.

```
ONIE:/ # mount /dev/sda2 /mnt/
```

b) Edit shadow file.

```
ONIE:/ # vi /mnt/etc/shadow
```

c) Remove 'admin' password.

Change the following line from:
admin:**1eE9WFgVk$EwGcNl83uK98.r8TcKn2q/**:15385:0:99999:7:::
into:
admin::15385:0:99999:7::: //Remove the string between the first and the second colon

d) Execute "**sync**" command.

```
ONIE:/ # sync
```

Step8 Repeat the steps from **a)** to **d)** in Step7 on */dev/sda3*.

The subsequent steps are distinguished between devices currently running in OVS and L2/L3 mode. Please choose the appropriate steps according to the PicOS mode.

Note: You can refer to the document Checking PicOS Mode to check the current PicOS mode of the device.

- If the running PicOS mode is L2/L3 mode, go to L2/L3 Mode.
- If the running PicOS mode is OVS mode, go to OVS Mode.

L2/L3 Mode:

Step9 Modify the configuration file.

```
ONIE:/# vi pica/config/pica_startup.boot
```

In the pica_startup.boot file, you will find lines starting with "***user admin {***", remove lines of user admin configurations.

For example, remove the following six lines in configuration file.

```
user admin {
            authentication {
                plain-text-password: "$1$zL8TUrpq$/Y1tcx1IhwPkm6HEd4aEM/"
            }
            class: "super-user"
        }
```

Save and exit with ":wq".

Copy the configuration file to the backup file.

```
ONIE:/# cp /mnt/pica/config/pica_startup.boot /mnt/backup/pica/config/pica_startup.boot
ONIE:/# sync
```

Step10 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step11 When you see PicOS login again, you can log in by the admin user without a password.

Step12 Set a new admin password using the following CLI commands and save the configuration.

```
root@XorPlus# set system login user admin authentication plain-text-password pica8            //Please enter the ne
root@XorPlus# set system login user admin class "super-user"
root@XorPlus# commit
```

After the above steps, you can log into the system with the new password.

OVS Mode：

Step9 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step10 Set a new admin password with **passwd admin** command and save the configuration. The commands are illustrated here:

```
root@XorPlus:~$ passwd admin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

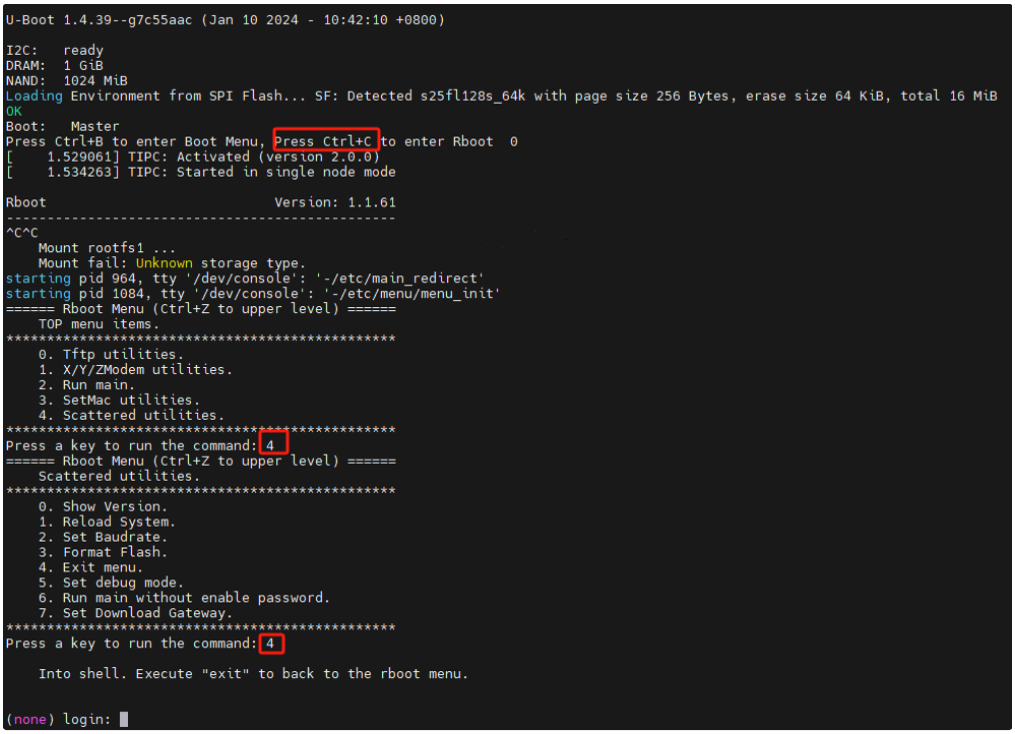
After the above steps, you can log into the system with the new password.

Password Recovery Guide for FS S5810/S5860 Series Switches

NOTEs:

- To enter the Rboot menu you need to reboot the device, which will lead to business interruption, so back up the device as needed, and perform password recovery at a time with less business.
- Before performing this operation, you need to contact the FS support at https://www.fs.com/tech_support.html to get the right *user name/password* used for entering Rboot shell.
- Do not power off the switch during this operation.

Step 1 Power off and on to force restarting the switch, then press **Ctrl+C** to enter Rboot menu.



Step 2 Type **4** in the Rboot menu to enter the *Scattered utilities* menu, then Type **4**, and enter the right user name and password to enter Rboot shell (Contact the FS support at

https://www.fs.com/tech_support.html to get the user name and password).

Step 3 At the Rboot shell, issue the following command to check whether the running system is PICOS or PICOS2 (used for determining the *config* file path described in the following steps).

```
root@(none):~# std_fw_printenv main
main=run picos_bootcmd
root@(none):~# std_fw_printenv main
main=run picos2_bootcmd
```

Step 4 Move the current configuration file.

```
root@(none):~# cd mnt/flash/picos/config1   // The path may be config1 or config2, this is up to the running system checked in step 3.
```

```
root@(none):/mnt/flash/picos/config1# mv latest.tar.gz latest_bak.tar.gz
root@(none):/mnt/flash/picos/config1# mv backup.tar.gz backup_bak.tar.gz
root@(none):/mnt/flash/picos/config1# sync
```

Step 5 Reboot the switch.

```
root@(none):~# reboot
```

Step 6 Since there are no configuration files in the */config1* directory, the switch boots to a factory default configuration. At this point you can log in as the **admin** user with the password **pica8**. Then use the following command to fetch your previous configuration.

```
admin@PICOS:~$ sudo su
root@PICOS:~$ cd  /mnt/open/picos/config1  // The path may be config1 or config2, this is up to the running system checked in step 3.
root@PICOS:~$ cp latest_bak.tar.gz latest.tar.gz
root@PICOS:~$ cp backup_bak.tar.gz backup.tar.gz
```

The subsequent steps distinguish between devices currently running in OVS mode or L2/L3 mode. For different modes, the steps are different.

- **OVS Mode**

Step 7 Modify the shadow file.

```
root@PICOS:~$ tar zxvf latest.tar.gz  etc/shadow
root@PICOS:~$ vi etc/shadow
```

In the shadow file, you will find one line starting with “admin:……..”. Here is an example:

```
admin:$1$eE9WFgVk$EwGcNl83uK98.r8TcKn2q/:15385:0:99999:7:::
```

You need to delete the letters between the first and the second colon and it will become:

```
admin::15385:0:99999:7:::
```

Step 8 Compress the shadow file to the configuration files and reboot**.**

```
root@PICOS:~$ gzip -d latest.tar.gz
root@PICOS:~$ tar -uf latest.tar etc/shadow
root@PICOS:~$ gzip latest.tar
root@PICOS:~$ sync
root@PICOS:~$ reboot -f
```

When you see the PICOS login again, you can log in as the admin user without a password.

Step 9 Login with username **admin**, and then set a new admin password and save the configuration. We can see that the OVS configuration has been restored.

```
PICOS-OVS login: admin
Linux PICOS-OVS 4.19.79 #1 SMP Sat Feb 17 03:04:25 CST 2024 armv7l
admin@PICOS-OVS:~$ passwd admin
New password:
Retype new password:
passwd: password updated successfully
admin@PICOS-OVS:~$ ovs-vsctl display-settings
ovs-vsctl add-br br0
ovs-vsctl set bridge br0  datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/2
ovs-vsctl set port ge-1/1/2  vlan_mode=trunk  tag=1
```

- **L2/L3 Mode**

Step 7 Under L2/L3 Mode, unzip and load the modified configuration file.

```
root@PICOS:/mnt/open/picos/config1#  tar zxvf latest.tar.gz  pica/config/pica_startup.boot
//The path may be config1 or config2, this is up to the running system checked in step 3.
```

```
root@PICOS# load override /mnt/open/picos/config1/pica/config/pica_startup.boot
root@PICOS# Loading config file...
Config file was loaded successfully.
root@PICOS# commit
```

Step 8 set a new admin password with CLI command and save the configuration.

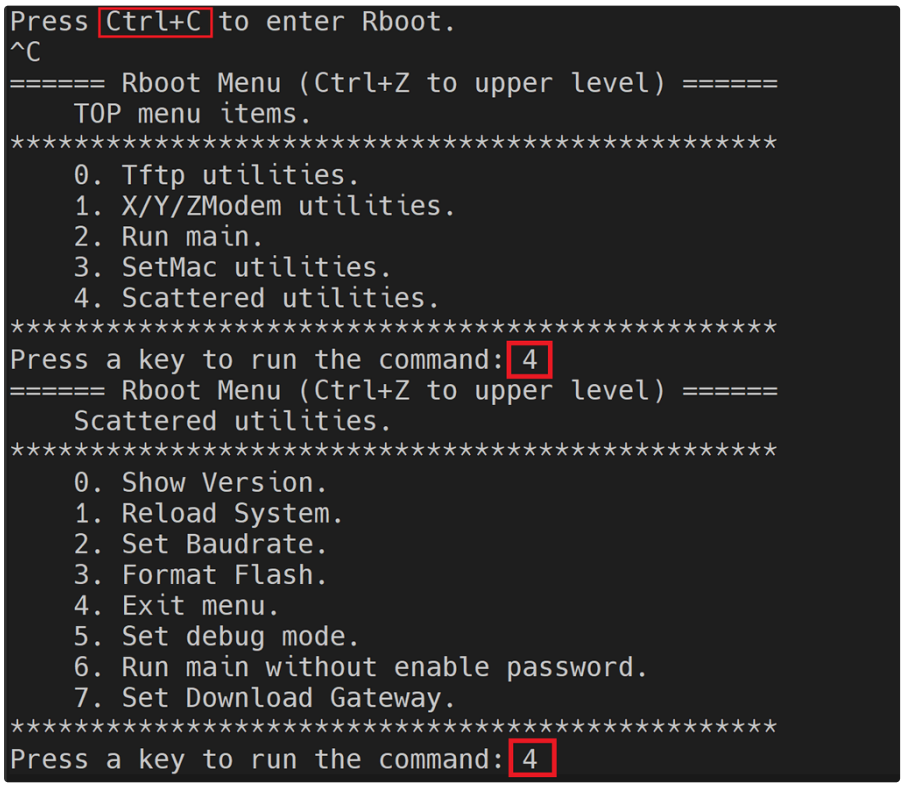
```
root@PICOS# set system login user admin authentication plain-text-password 12345678
root@PICOS# commit
root@PICOS# run copy running-config startup-config
```

Password Recovery Guide for FS N8560-32C

NOTEs:

- To enter the Rboot menu you need to reboot the device, which will lead to business interruption, so back up the device as needed, and perform password recovery at a time with less business.
- Before performing this operation, you need to contact the FS support at https://www.fs.com/tech_support.html to get the right *user name/password* used for entering Rboot shell.
- Do not power off the switch during this operation.

Step 1 Power off and on to force restarting the switch, then press **Ctrl+C** to enter Rboot menu.



Step 2 Type **4** in the Rboot menu to enter the *Scattered utilities* menu, then Type **4**, and enter the right user name and password to enter Rboot shell (Contact the FS support at

https://www.fs.com/tech_support.html to get the user name and password).

Step3 Check out the PICOS system boot partition.

```
ONIE:/ # blkid
/dev/sda6: LABEL="User-Data" UUID="da55e09c-0e7b-4d96-a8c9-bee2ed5bb42c"
/dev/sda5: LABEL="PicOS2" UUID="3f228548-64c1-492c-ad3d-8ca7d248c11a"
/dev/sda4: LABEL="PicOS" UUID="039453f9-0879-4c86-9e0b-8ef4d34d9a66"
/dev/sda3: LABEL="PICOS-GRUB" UUID="b3a8ab95-43f9-4f21-9c76-7f48101be381"
/dev/sda2: LABEL="ONIE-BOOT" UUID="7fcaa6c8-d174-42c1-abd1-8c6eea46eb6b"
/dev/sda1: LABEL="EFI System" UUID="36E9-D2F5"
ONIE:/ #
```

We find that the partition of **LABEL="PicOS2"** is **/dev/sda5** and **LABEL="PicOS"** is **/dev/sda4**.

Step4 From the ONIE prompt, perform the following commands to mount the boot partition.

```
ONIE:/ # mount /dev/sda5 /mnt/
ONIE:/ # mount /dev/sda4 /mnt/
```

Step5 Modify the shadow file.

```
# vi etc/shadow
```

Change the following line from:
admin:**1eE9WFgVk$EwGcNl83uK98.r8TcKn2q/**:15385:0:99999:7:::
into:
admin::15385:0:99999:7::: //Remove the string between the first and the second colon

Step6 Execute the sync operation.

```
# sync
```

The subsequent steps are distinguished between devices currently running in OVS and L2/L3 mode. Please choose the appropriate steps according to the PicOS mode.

L2/L3 Mode:

Step7 Modify the configuration file.

```
ONIE:/# vi pica/config/pica_startup.boot
```

In the pica_startup.boot file, you will find lines starting with "***user admin {***", remove lines of user admin configurations.

For example, remove the following six lines in configuration file.

```
user admin {
            authentication {
                plain-text-password: "$1$zL8TUrpq$/Y1tcx1IhwPkm6HEd4aEM/"
            }
            class: "super-user"
        }
```

Save and exit with ":wq".

Copy the configuration file to the backup file.

```
ONIE:/# cp /mnt/pica/config/pica_startup.boot /mnt/backup/pica/config/pica_startup.boot
ONIE:/# sync
```

Step8 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step9 When you see PicOS login again, you can log in by the admin user without a password.

Step10 Set a new admin password using the following CLI commands and save the configuration.

```
root@XorPlus# set system login user admin authentication plain-text-password pica8           //Please enter
the new password
root@XorPlus# set system login user admin class "super-user"
root@XorPlus# commit
```

After the above steps, you can log into the system with the new password.

OVS Mode：

Step7 Umount and reboot the switch.

```
# umount /mnt
# reboot
```

Step8 Set a new admin password with **passwd admin** command and save the configuration. The commands are illustrated here:

```
root@XorPlus:~$ passwd admin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

After the above steps, you can log into the system with the new password.

Setting Date and Time

This section describes how to set the time zone, date, and time.

Setting Time Zone

To see the current time zone, list the contents of the **/etc/timezone** directory.

```
admin@Switch$cat /etc/timezone
Etc/UTC
```

To set the time zone, run the **dpkg-reconfigure tzdata** command as root.

```
admin@Switch$sudo dpkg-reconfigure tzdata
Package configuration
  +----------------------------------+ Configuring tzdata +-----------------------------------+
  | Please select the geographic area in which you live. Subsequent configuration questions     |
  | will narrow this down by presenting a list of cities, representing the time zones in which  |
  | they are located.                                                                           |
  |                                                                                             |
  | Geographic area:                                                                            |
  |                                                                                             |
  |                                      Africa                                                 |
  |                                      America                                                |
  |                                      Antarctica                                             |
  |                                      Australia                                              |
  |                                      Arctic                                                 |
  |                                      Asia                                                   |
  |                                      Atlantic                                               |
  |                                      Europe                                                 |
  |                                      Indian                                                 |
  |                                      Pacific                                                |
  |                                      SystemV                                                |
  |                                      US                                                     |
  |                                      Etc                                                    |
  |                                                                                             |
  |                                                                                             |
  |                          <Ok>                              <Cancel>                         |
  |                                                                                             |
  +---------------------------------------------------------------------------------------------+
```

Navigate through the menus to set the appropriate time zone.

```
+-----------------------+ Configuring tzdata +-----------------------+
| Please select the city or region corresponding to your time zone.  |
|                                                                    |
| Time zone:                                                         |
|                                                                    |
|                           Alaska                                   |
|                           Aleutian                                 |
|                           Arizona                                  |
|                           Central                                  |
|                           Eastern                                  |
|                           Hawaii                                   |
|                           Indiana-Starke                           |
|                           Michigan                                 |
|                           Mountain                                 |
|                           Pacific                                  |
|                           Pacific-New                              |
|                           Samoa                                    |
|                                                                    |
|                                                                    |
|                 <Ok>                    <Cancel>                   |
|                                                                    |
+--------------------------------------------------------------------+
```

Then, the selected time zone should be displayed.

```
Current default time zone: 'US/Eastern'
Local time is now:      Mon Dec  7 21:15:30 EST 2015.
Universal Time is now:  Tue Dec  8 02:15:30 UTC 2015.
```

Verify if the time zone is correctly set.

```
admin@Switch$cat /etc/timezone
US/Eastern
```

Setting Date and Time

The switch has a hardware clock that maintains system time, even when the switch is rebooted or powered off. The hardware clock is powered by a battery on the system board. When the switch is running, PicOS maintains its own software clock. During switch boot up, the hardware clock is copied to the software clock maintained by PicOS. The software clock is then referenced for anything that requires time keeping. During switch shut down, the software clock is copied back to the hardware clock.

To set the date and time on the software clock, use the **date** command as root.

```
admin@Switch$sudo date --set 2015-12-07
Mon Dec  7 00:00:00 EST 2015
admin@Switch$sudo date --set 13:21:00
Mon Dec  7 13:21:00 EST 2015
```

To display the current date and time, use the **date** command without arguments.

```
admin@Switch$date
Mon Dec  7 13:23:00 EST 2015
```

To set the date and time on the hardware clock, use the **hwclock** command as root.

Boot Diagnosis Report

There is a report to diagnose whether all hardwares are good during switch power on.

Diagnosis content are as below:

1. Version

(1) Show system version

(2) Show ONIE version

(3) Show CPLD version

2. Hardware information

(1) Manage port mac address

(2) System mac address

(3) Board serial number

(4) Board product name

3. PSU

(1) PSU present

(2) PSU power good

(3) PSU serial number (verizon no sn)

4. FAN

(1) FAN fault bit

(2) Fan speed less than 15% error (1200rpm)

5. Temperature

(1) CPU temperature

(2) Switch chip temperature

(3) Board temperature

Warning when environmental temperature more than 60 C!

6. Detect optical module

(1) Detect plugged in

(2) Show vendor name

(3) Show vendor sn

(4) Show optical type (verizon no)

7. RTC

(1) Read time form RTC

(2) Show read time

8. Disk space

(1) Show all disk size

(2) Show PicOS free disk space

(3) Warning when free space Less than 10%

9. Memory size

(1) Total memory size

(2) Free memory size

10. CPU utilization

11. POE module

(1) PoE status

Location of report file

```
admin@XorPlus> start shell sh
admin@XorPlus$vi /var/log/report_diag.log
************ PicOS Diagnosis Start ************
Date: Thu Dec 22 18:00:29 UTC 2016
Version:
    Copyright (C) 2009-2016 Pica8, Inc.
```

```
    ============================
    Hardware Model                : as4610_30t
    Linux System Version/Revision : 2.0.6/904f28d
    Linux System Released Date    : 12/22/2016
    L2/L3 Version/Revision        : 2.0.6/904f28d
    L2/L3 Released Date           : 12/22/2016
    OVS/OF Version/Revision       : 2.0.6/904f28d
    OVS/OF Released Date          : 12/22/2016
    ONIE version    : master-201508292125.2.5.4-dirty
    CPLD version    : CPLD version V0.2
Hardware information:
    MAC address    : 00:90:4C:06:A5:72
    Serial number    : SN1234567
    Product name    : 4610-30T-O-AC-F
PSU:
    PSU 1 status    : present but power off
    PSU 2 status    : present and power on
System FAN:
    There is no FAN in box
Temperature:
    CPU temperature        : 45 C / 113 F
    Switch chip temperature    : 45 C / 113 F
    Board temperature    : 45 C / 113 F
Optical modules:
    Port 1 Module type: SFP; Vendor name: OEM; Serial number: A85351050279
    Port 2 Module type: SFP; Vendor name: FINISAR; Serial number: P117EWY
    Port 3 Module type: SFP; Vendor name: OEM; Serial number: A85351050293
    Port 4 Module type: SFP; Vendor name: AVAGO; Serial number: AD0834A00LU
    Port 5 no module
    Port 6 no module
RTC:
    RTC test ok
    Time    : Thu Dec 22 18:00:30 2016  -0.435949 seconds
Disk space:
    /dev/sda    : 7676 MB
    /dev/sda1    : 1500 MB
    /dev/sda2    : 600 MB
    /dev/sda3    : 1500 MB    (Rootfs)
    Free size of rootfs partition is 577 MB.
Memory size:
    Total memory    : 765008 KB
    Free memory    : 536476 KB
CPU utilization: 8.90%
POE module:  OK
************  PicOS Diagnosis End  ************
```

Diagnosis command

This command can be used after switch power on. The content of report will append the report_diag.log file for every time diagnosis.

```
admin@XorPlus$sudo su
root@XorPlus$system-diag
************ PicOS Diagnosis Start ************
Date: Thu Dec 29 16:43:14 UTC 2016
Version:
    Copyright (C) 2009-2016 Pica8, Inc.
    ==================================
    Hardware Model                : as4610_30p
    Linux System Version/Revision : 2.7.2S1D/dc2173f
    Linux System Released Date    : 12/28/2016
    L2/L3 Version/Revision        : 2.7.2S1D/dc2173f
    L2/L3 Released Date           : 12/28/2016
    OVS/OF Version/Revision       : 2.7.2S1D/dc2173f
    OVS/OF Released Date          : 12/28/2016
    ONIE version    : master-201508292125.2.5.4-dirty
    CPLD version    : CPLD version V0.2
Hardware information:
    MAC address : 70:72:CF:FD:8F:20
    Serial number   : AF10029779
```

```
    Product name    : 4610-30P-O-AC-F
PSU:
    PSU 1 status    : present but power off
    PSU 2 status    : present and power on
System FAN:
    Fan 1 fault
Temperature:
    CPU temperature     : 35 C / 95 F
    Switch chip temperature : 35 C / 95 F
    Board temperature   : 35 C / 95 F
Optical modules:
    Port 1 no module
    Port 2 no module
    Port 3 no module
    Port 4 no module
    Port 5 no module
    Port 6 no module
RTC:
    RTC is OK
    Time    : Thu Dec 29 16:43:16 2016  -0.470233 seconds
Disk space:
    /dev/sda    : 7676 MB
    /dev/sda1   : 256 MB
    /dev/sda2   : 1500 MB   (Rootfs)
    /dev/sda3   : 600 MB
    Free size of rootfs partition is 930 MB.
Memory size:
    Total memory    : 2057300 KB
    Free memory : 1826960 KB
CPU utilization: 13.83%
POE module:  OK
************  PicOS Diagnosis End  ************
```

Rebooting the System

Rebooting the System

```
admin@XorPlus>request system reboot
U-Boot 1.3.0 (Apr 11 2011 - 10:41:10)
CPU: 8541, Version: 1.1, (0x80720011)
Core: E500, Version: 2.0, (0x80200020)
Clock Configuration:
CPU: 825 MHz, CCB: 330 MHz,
DDR: 165 MHz, LBC: 41 MHz
L1: D-cache 32 kB enabled
I-cache 32 kB enabled
I2C: ready
DRAM: Initializing
DDR: 512 MB
FLASH: 32 MB
L2 cache 256KB: enabled
Set ethaddr MAC address = 60:eb:69:d2:9c:d8
In: serial
Out: serial
Err: serial
Net: TSEC0
IDE: Bus 0: OK
Device 0: Model: TRANSCEND Firm: 20091130 Ser#: 20100723 C4130E83
Type: Hard Disk
Capacity: 1911.6 MB = 1.8 GB (3915072 x 512)
```

Auto-Run Script Upon System Boot Up

From PicOS2.9.1, user can add customized scripts which will run automatically upon system boot up.

The script at **/cftmp/auto/pre-nos** will be started when Linux booting is over. The script at **/cftmp/auto/post-xorplus** will be launched when XorPlus is ready. And the script at **/cftmp/auto/post-ovs** will be launched when OVS is ready.

The files **pre-nos/ post-xorplus/ post-ovs** are not existing in directory **/cftmp/auto** defaultly. If user want to run the scripts, they need to create them and make sure they are read and write files.

Example 1:

Run script when Linux booting over.

```
admin@PicOS-OVS$sudo touch /cftmp/auto/pre-nos
admin@PicOS-OVS$sudo chmod 777 /cftmp/auto/pre-nos
admin@PicOS-OVS$sudo vi /cftmp/auto/pre-nos
echo "####################Start add linux scripts####################"
echo "####################Add linux scripts finished####################"

admin@PicOS-OVS$sudo reboot
...
...
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
####################Start add linux scripts####################
####################Add linux scripts finished####################
Auto Provisioning Tool - checking updates ....
No tftp server address found, exit now
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Stopping internet superserver: xinetd.
[ ok ] Restarting OpenBSD Secure Shell server: sshd.
[ ok ] Create Inventory database file.
[ ok ] Starting web server: lighttpd.
[ ok ] Starting network snmp: snmpd.
[....] Starting: Open vSwitch/OpenFlowdevice ovs-pica8 entered promiscuous mode
device br0 entered promiscuous mode
. ok

OVS login:
```

Example 2:

Run script when OVS is ready.

```
admin@PicOS-OVS$sudo touch /cftmp/auto/post-ovs
admin@PicOS-OVS$sudo chmod 777 /cftmp/auto/post-ovs
admin@PicOS-OVS$sudo vi /cftmp/auto/post-ovs
echo "Start add ovs scripts"
ovs-vsctl del-br br0
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1
ovs-vsctl add-port br0 te-1/1/2
ovs-vsctl add-port br0 te-1/1/3
ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:2,bucket=output:3
ovs-ofctl add-meter br0 meter=1,kbps,stats,band=type=drop,rate=10000
ovs-ofctl add-flow br0 in_port=1,actions=meter:1,group:1
echo "Add ovs scripts finished"

admin@PicOS-OVS$sudo systemctl restart picos
```

```
.........................
```

Example 3:

Run script when Xorplus is ready.

```
admin@XorPlus$sudo touch /cftmp/auto/post-xorplus
admin@XorPlus$sudo chmod 777 /cftmp/auto/post-xorplus
admin@XorPlus$sudo vi /cftmp/auto/post-xorplus
echo "Start add xorplus scripts"
/usr/bin/cli -c 'configure;
set interface gigabit-ethernet te-1/1/1 crossflow enable true;
set interface gigabit-ethernet te-1/1/1 crossflow local-control false;
set interface gigabit-ethernet te-1/1/2 crossflow enable true;
set interface gigabit-ethernet te-1/1/2 crossflow local-control false;
set interface gigabit-ethernet te-1/1/3 crossflow enable true;
set xovs enable true;
commit'
ovs-vsctl del-br br0
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1
ovs-vsctl add-port br0 te-1/1/2
ovs-vsctl add-port br0 te-1/1/3 -- set interface te-1/1/3 type=crossflow
ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:2,bucket=output:3
ovs-ofctl add-meter br0 meter=1,kbps,stats,band=type=drop,rate=10000
ovs-ofctl add-flow br0 in_port=1,actions=meter:1,group:1
echo "Add xorplus scripts finished"


admin@PicOS-OVS$sudo systemctl restart picos
.........................
root@XorPlus>
Execute command: configure.
Entering configuration mode.
There are no other users in configuration mode.
root@XorPlus#
Execute command:
set interface gigabit-ethernet te-1/1/1 crossflow enable true.
root@XorPlus#
Execute command:
set interface gigabit-ethernet te-1/1/1 crossflow local-control false.
root@XorPlus#
Execute command:
set interface gigabit-ethernet te-1/1/2 crossflow enable true.
root@XorPlus#
Execute command:
set interface gigabit-ethernet te-1/1/2 crossflow local-control false.
root@XorPlus#
Execute command:
set interface gigabit-ethernet te-1/1/3 crossflow enable true.
root@XorPlus#
Execute command:
set xovs enable true.
root@XorPlus#
Execute command:
commit
.
Commit OK.
Save done.
root@XorPlus#
ovs-vsctl: no bridge named br0
device ovs-pica8 entered promiscuous mode
device br0 entered promiscuous mode
Add xorplus scripts finished
admin@XorPlus$
```

Sample for Crossflow OVS Remarking Rules with Auto-run Script

NOTE:

Do not use Microsoft txt editors to create your post-ovs file as these include extra formatting which cannot be understood by PICOS. Use only Linux editors.

In the examples below, you can copy and paste these commands to your switch and these commands will create the bridge and add the ports to the bridge. Be sure to change the interface names depending on your specific switch model; as an example ge-1/1/1 or te-1/1/1 etc.

Step1 From the CLI, enable Crossflow and create the ovs-vswitchd.conf.

```
admin@AS5812-54X-SwitchA# set xovs enable true
admin@AS5812-54X-SwitchA# commit
```

Step2 Configure the ports to be Crossflow ports.

```
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/3 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/4 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/5 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/6 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/7 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/8 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/9 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/10 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/11 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/12 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/13 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/14 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/15 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/15 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/16 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/17 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/18 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/19 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/20 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/21 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/22 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/23 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/24 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/25 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/26 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/27 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/28 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/29 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/30 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/31 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/32 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/33 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/34 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/35 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/36 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/37 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/38 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/39 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/40 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/41 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/42 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/43 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/44 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/45 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/46 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/47 crossflow enable true
admin@AS5812-54X-SwitchA# set interface gigabit-ethernet te-1/1/48 crossflow enable true
```

Step3 Verify that the ovs-vSwitch DB is present.

```
admin@AS5812-54X-SwitchA# run bash "start shell sh"
admin@AS5812-54X-SwitchA:/$ cd /ovs
admin@AS5812-54X-SwitchA:/ovs$ ls
ovs-vswitchd.conf.db
admin@AS5812-54X-SwitchA:/ovs$ ovs-vsctl show
9c0bd1cb-a65f-4fa1-8c16-4cc045319984
```

Step4 Create a bridge and add interfaces to it:

```
admin@AS5812-54X-SwitchA:/ovs$ ovs-vsctl add-br br0
```

Step5 Add ports to the bridge.

```
ovs-vsctl add-port br0 te-1/1/1 -- set interface te-1/1/1 type=crossflow
ovs-vsctl add-port br0 te-1/1/2 -- set interface te-1/1/2 type=crossflow
ovs-vsctl add-port br0 te-1/1/3 -- set interface te-1/1/3 type=crossflow
ovs-vsctl add-port br0 te-1/1/4 -- set interface te-1/1/4 type=crossflow
ovs-vsctl add-port br0 te-1/1/5 -- set interface te-1/1/5 type=crossflow
ovs-vsctl add-port br0 te-1/1/6 -- set interface te-1/1/6 type=crossflow
ovs-vsctl add-port br0 te-1/1/7 -- set interface te-1/1/7 type=crossflow
ovs-vsctl add-port br0 te-1/1/8 -- set interface te-1/1/8 type=crossflow
ovs-vsctl add-port br0 te-1/1/9 -- set interface te-1/1/9 type=crossflow
ovs-vsctl add-port br0 te-1/1/10 -- set interface te-1/1/10 type=crossflow
ovs-vsctl add-port br0 te-1/1/11 -- set interface te-1/1/11 type=crossflow
ovs-vsctl add-port br0 te-1/1/12 -- set interface te-1/1/12 type=crossflow
ovs-vsctl add-port br0 te-1/1/13 -- set interface te-1/1/13 type=crossflow
ovs-vsctl add-port br0 te-1/1/14 -- set interface te-1/1/14 type=crossflow
ovs-vsctl add-port br0 te-1/1/15 -- set interface te-1/1/15 type=crossflow
ovs-vsctl add-port br0 te-1/1/16 -- set interface te-1/1/16 type=crossflow
ovs-vsctl add-port br0 te-1/1/17 -- set interface te-1/1/17 type=crossflow
ovs-vsctl add-port br0 te-1/1/18 -- set interface te-1/1/18 type=crossflow
ovs-vsctl add-port br0 te-1/1/19 -- set interface te-1/1/19 type=crossflow
ovs-vsctl add-port br0 te-1/1/20 -- set interface te-1/1/20 type=crossflow
ovs-vsctl add-port br0 te-1/1/21 -- set interface te-1/1/21 type=crossflow
ovs-vsctl add-port br0 te-1/1/22 -- set interface te-1/1/22 type=crossflow
ovs-vsctl add-port br0 te-1/1/23 -- set interface te-1/1/23 type=crossflow
ovs-vsctl add-port br0 te-1/1/24 -- set interface te-1/1/24 type=crossflow
ovs-vsctl add-port br0 te-1/1/25 -- set interface te-1/1/25 type=crossflow
ovs-vsctl add-port br0 te-1/1/26 -- set interface te-1/1/26 type=crossflow
ovs-vsctl add-port br0 te-1/1/27 -- set interface te-1/1/27 type=crossflow
ovs-vsctl add-port br0 te-1/1/28 -- set interface te-1/1/28 type=crossflow
ovs-vsctl add-port br0 te-1/1/29 -- set interface te-1/1/29 type=crossflow
ovs-vsctl add-port br0 te-1/1/30 -- set interface te-1/1/30 type=crossflow
ovs-vsctl add-port br0 te-1/1/31 -- set interface te-1/1/31 type=crossflow
ovs-vsctl add-port br0 te-1/1/32 -- set interface te-1/1/32 type=crossflow
ovs-vsctl add-port br0 te-1/1/33 -- set interface te-1/1/33 type=crossflow
ovs-vsctl add-port br0 te-1/1/34 -- set interface te-1/1/34 type=crossflow
ovs-vsctl add-port br0 te-1/1/35 -- set interface te-1/1/35 type=crossflow
ovs-vsctl add-port br0 te-1/1/36 -- set interface te-1/1/36 type=crossflow
ovs-vsctl add-port br0 te-1/1/37 -- set interface te-1/1/37 type=crossflow
ovs-vsctl add-port br0 te-1/1/38 -- set interface te-1/1/38 type=crossflow
ovs-vsctl add-port br0 te-1/1/39 -- set interface te-1/1/39 type=crossflow
ovs-vsctl add-port br0 te-1/1/40 -- set interface te-1/1/40 type=crossflow
ovs-vsctl add-port br0 te-1/1/41 -- set interface te-1/1/41 type=crossflow
ovs-vsctl add-port br0 te-1/1/42 -- set interface te-1/1/42 type=crossflow
ovs-vsctl add-port br0 te-1/1/43 -- set interface te-1/1/43 type=crossflow
ovs-vsctl add-port br0 te-1/1/44 -- set interface te-1/1/44 type=crossflow
ovs-vsctl add-port br0 te-1/1/45 -- set interface te-1/1/45 type=crossflow
ovs-vsctl add-port br0 te-1/1/46 -- set interface te-1/1/46 type=crossflow
ovs-vsctl add-port br0 te-1/1/47 -- set interface te-1/1/47 type=crossflow
ovs-vsctl add-port br0 te-1/1/48 -- set interface te-1/1/48 type=crossflow
```

Step6 Create a bond to treat all access interfaces as same:

```
ovs-vsctl add-port br0 bond1 -- set interface bond1 type=pica8_bond
ovs-vsctl set interface bond1 options:members=te-1/1/1,te-1/1/2,te-1/1/3,te-1/1/4,te-1/1/5,te-1/1/6,te-1/1/7,te-1/
```

Step7 Set OVS to be able to match the VLAN number.

```
ovs-vsctl set-option-match-vlan-type true > /dev/null
```

Step8 Reboot the switch.

```
admin@AS5812-54X-SwitchA$sudo systemctl restart picos
```

NOTE:

- We must reboot the switch to leverage the above feature.
- When using OF rules to direct traffic and remark the DSCP values, bridge and interfaces must already be configured and found within the OVS vSwitchd database as shown be. This configuration of bridges and interfaces only has to be done once. These configurations are automatically saved to the vSwitch database.

Step9 The attached file test-flows.txt which will be the new post-ovs after you edit it and copy it to the /cftmp/auto directory and rename it to post-ovs. You need to change the mode to executable via the following command.

```
admin@AS5812-54X-SwitchA$sudo chmod 777 /cftmp/auto/post-ovs
```

test-flows.txt :



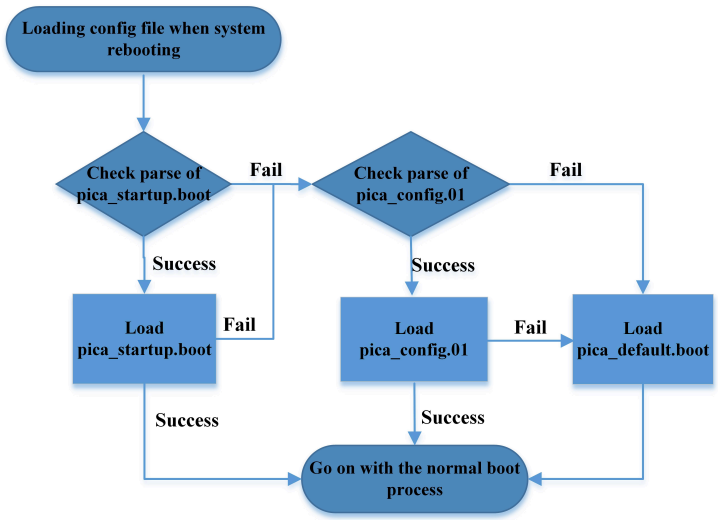
Graceful Bootup with Backup Configuration

When the system's configuration file ***pica_startup.boot*** is damaged due to incorrect configuration, the system will fail to startup. PICA8 provides a feature of Graceful Bootup with Backup Configuration to solve this problem. It ensures the device boots up properly and with the backup configuration file *pica.conf* when startup configuration file ***pica_startup.boot*** is damaged due to incorrect configuration.

pica.conf is a backup of the ***pica_startup.boot*** file which is saved in directory */pica/config*. When the user commits a configuration successfully, the system automatically saves the configuration to the ***pica_startup.boot*** file and synchronizes the configuration to the ***pica.conf*** file. In the event of an upgrade, the upgraded system will retain the previous ***pica_startup.boot***, and the ***pica.conf*** file is a copy of ***pica_startup.boot*** file. But in the case of newly installed image, the system will not have the **pica_startup.boot**, and the ***pica.conf*** file is a copy of ***pica_default.boot*** file. The boot process is further explained below.

Process of Loading Configuration File

Figure 1 Process of loading configuration file when system rebooting



As shown in **Figure 1**, the process of loading configuration file when system rebooting is as follows:

1. The system starts loading the configuration file by parsing the ***pica_startup.boot*** file to the syntax.
   - If the result of the check is success, system will load ***pica_startup.boot*** file, go to step 2.
   - If the result of the check is fail, that is, the ***pica_startup.boot*** file is damaged, the system will check the syntax of ***pica.conf***, and a syslog message is provided, go to step 3.
2. Load ***pica_startup.boot*** file.
   - If load ***pica_startup.boot*** file successfully, it will go on with the normal boot process.
   - If failed to load ***pica_startup.boot*** file, the system will check the syntax of ***pica.conf***, and a syslog message is provided, go to step 3.
3. Check the syntax of ***pica.conf*** file.
   - If the result of the check is success, the system will load ***pica.conf*** file, go to step 4.
   - If the result of the check is fail, that is, the ***pica.conf*** file is damaged, the system will load ***pica_default.boot*** file, and a syslog message is provided, go to step 5.
4. Load ***pica.conf*** file.
   - If load ***pica.conf***file successfully, it will go on with the normal boot process.
   - If failed to load ***pica.conf*** file, the system will load ***pica_default.boot*** file, and a syslog message is provided, go to step 5.
5. Load ***pica_default.boot*** file in directory */pica/etc/platform_name (*For example, on AS5712_54X, **pica_default.boot** file is in the */pica/etc/as5712_54x* directory*)*, and go on with the normal boot process.

IP Rule of Management Network and Service Network

- Introduction
  - Usage of IP Rule
  - Policy Routing Rules
- Example

Introduction

IP rule is a policy routing function of Linux systems. Compared with the classic routing algorithms used on the internet that make routing decisions based only on the destination address of packets, IP rule is more flexible which can support more filter attributes for route forwarding. IP rule can select routes by executing some set of policy routing rules and could set priorities of the rules.

Usage of IP Rule

```
Usage: ip rule [ list | add | del ] SELECTOR ACTION
SELECTOR := [ from PREFIX ] [ to PREFIX ] [ tos TOS ][ dev STRING ] [ pref NUMBER ]
ACTION := [ table TABLE_ID ] [ nat ADDRESS ][ prohibit | reject | unreachable ]
                [ flowid CLASSID ]
TABLE_ID := [ local | main | default | new | NUMBER ]
```

IP rule supports configuring **SELECTOR** of the following attributes for choosing a forwarding path:

From - source address

To - destination address (here we can choose the rules, also used to search the routing entry)

Tos - TOS (type of sevice) field in IP header

Dev - physical interface

Fwmark - firewall parameters

IP rule supports configuring the **ACTION** on how to process the packets if the rule selector matches:

Table - the routing table identifier to lookup if the rule selector matches

Nat - translate the source address of the IP packet into some other value

Prohibit - drop the packets and generate a 'Communication is administratively prohibited' error
Reject - drop the packets

Unreachable - drop the packets and generate a 'Network is unreachable' error

Policy Routing Rules

Linux supports up to 255 routing tables, each routing table has its own table name and table ID. IP rule action defines tables to lookup if the rule selector matches. IP rule also defines the priority parameter which indicates the priority of this rule. Higher number means lower priority, and rules get processed in order of increasing number. Each rule should have an explicitly set unique priority value.

When executing **ip rule** command on Linux shell, we can find all the IP rules of the current system.

```
admin@Xorplus$ip rule
1000:  from all lookup [l3mdev-table]
1500:  from all lookup local
2000:  from 10.10.51.142 lookup main
2001:  from all to 10.10.51.142/24 lookup main
2010:  from all lookup 252
32766: from all lookup main
32767:  from all lookup default
```

By default, the kernel has three rules setting:

- Priority: 1500, Selector: match anything, Action: lookup routing table **local** (ID 255). The local table is a special routing table containing high priority control routes for local and broadcast addresses.
- Priority: 32766, Selector: match anything, Action: lookup routing table **main** (ID 254). The main table is the normal routing table containing all non-policy routes and all the management network routes.
- Priority: 32767, Selector: match anything, Action: lookup routing table **default** (ID 253). The default table is empty. It is reserved for some post-processing if no previous default rules selected the packet.

On the basis of the default rules, PICOS adds three new rules before the rule with priority 32766.

- Priority: 1000, Selector: match anything, Action: lookup routing table **l3mdev-table**. The **l3mdev-table** is a VRF associated routing table.

- Priority: 2000, Selector: match packets from all source to destination address of **eth0_subnet**, Action: lookup routing table main (ID 254). The **eth0_subnet** represents the subnet address of eth0 interface, for example, if the IP address of eth0 interface is 10.10.51.195, then eth0_subnet will be 10.10.51.195/24.
- Priority: 2001, Selector: match from source address of packets **eth0_address**, Action: lookup routing table **main** (ID 254). The **eth0_address** represents the IP address of eth0 interface, for example, 10.10.51.195.
- Priority: 2010, Selector: match anything, Action: lookup routing table **252** (ID 252, both table name and table ID are 252). The **252** table contains all the IPv4 service network routes.

NOTE:

- If data packets match the routes in both 252 table and main table, the routing table entries in 252 table are used preferentially for route forwarding as the priority of 252 table is higher than the main table.
- 252 table only supports IPv4 routing entries, IPv6 routing entries are still in the main table.

Example

Here is an example explaining how IP rule works on management network routes and service network routes.

1. Configure IP addresses for service port and eth0 management port.

   #Configure the IP address for service port.

```
admin@Xorplus# set vlans vlan-id 3
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 3
admin@Xorplus# set l3-interface vlan-interface vlan-3 address 192.168.2.1 prefix-length 24
admin@Xorplus# set vlans vlan-id 3 l3-interface vlan-3
admin@Xorplus# commit
Commit OK.
Save done.
```

   #Assign an IP address to the eth0 management port by default method of DHCP. Use **ifconfig eth0** command to find the IP address of eth0.

```
admin@Xorplus$ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:18:23:30:dd:52
          inet addr:10.10.51.142  Bcast:10.10.51.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6866 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:889873 (869.0 KiB)  TX bytes:200121 (195.4 KiB)
```

2. Configure the next hop of 10.10.20.0/24 as the IP address of the service network segment.

```
admin@Xorplus# set protocols static route 10.10.20.0/24 next-hop 192.168.2.5
admin@Xorplus# commit
Commit OK.
Save done.
```

Check the routing table. The above routing entry is only in 252 table and not in the main table because the next hop is the IP address of the service network segment.

```
admin@Xorplus# run show route ipv4
IPv4 Routing table: 3 routes
10.10.20.0/24      [static(1)/1]
                   > to 192.168.2.5 via vlan-3/vlan-3
192.168.2.1/32     [local(0)/0]
                   > via vlan-3/vlan-3
192.168.2.0/24     [connected(0)/0]
                   > via vlan-3/vlan-3
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C>* 10.10.51.0/24 is directly connected, eth0, 01:33:30
S>* 10.10.20.0/24 [1/0] via 192.168.2.5, vlan3, weight 1, 01:05:18
C>* 192.168.2.0/24 is directly connected, vlan3, 01:05:18
admin@Xorplus# quit
admin@Xorplus> quit
```

```
admin@Xorplus$ip route list table 252
10.10.20.0/24 via 192.168.2.5 dev vlan.3  proto xorp  metric 1
192.168.2.0/24 via 192.168.2.1 dev vlan.3  proto xorp

root@Xorplus$ip route list table main
default via 10.10.51.1 dev eth0
10.10.51.0/24 dev eth0  proto kernel  scope link  src 10.10.51.142
192.168.2.0/24 dev vlan.3  proto kernel  scope link  src 192.168.2.1
```

3. Configure next hop of default route as IP address of the management network gateway.

> **NOTE:**
>
> The management port does not support the configuration of network segment routing, you can only configure the default route.

```
admin@Xorplus# set protocols static route 0.0.0.0/0 next-hop 10.10.51.1
admin@Xorplus# commit
Commit OK.
Save done.
```

Check the routing table. The above routing entry is only in main table and not in 252 table because the next hop is the IP address of the management network segment.

```
admin@Xorplus$ip route list table main
default via 10.10.51.1 dev eth0
10.10.51.0/24 dev eth0  proto kernel  scope link  src 10.10.51.142
192.168.2.0/24 dev vlan.3  proto kernel  scope link  src 192.168.2.1

admin@Xorplus$ip route list table 252
10.10.20.0/24 via 192.168.2.5 dev vlan.3  proto xorp  metric 1
192.168.2.0/24 via 192.168.2.1 dev vlan.3  proto xorp
```

4. Configure the next hop of default route as the IP address of the service network segment.

```
admin@Xorplus# set protocols static route 0.0.0.0/0 next-hop 192.168.2.88
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# quit
admin@Xorplus> quit
```

Check the routing table. The above routing entry is only in 252 table and not in main table because the next hop is the IP address of the service network segment.

```
admin@Xorplus$ip route list table 252
default via 192.168.2.88 dev vlan.3  proto xorp  metric 1
10.10.20.0/24 via 192.168.2.5 dev vlan.3  proto xorp  metric 1
192.168.2.0/24 via 192.168.2.1 dev vlan.3  proto xorp

admin@Xorplus$ip route list table main
default via 10.10.51.1 dev eth0
10.10.51.0/24 dev eth0  proto kernel  scope link  src 10.10.51.142
192.168.2.0/24 dev vlan.3  proto kernel  scope link  src 192.168.2.1
```

There are default routing entries in both 252 table and main table, the default routing entry in the main table is automatically generated by the system when assigning the IP address by DHCP. When the packet matches no routing entry in the routing table, it will then match the default routing entry. In this case, the default routing entry in 252 table is used preferentially for route forwarding as the priority of 252 table is higher than the main table.

5. If the source IP address carried in a packet is empty and the packet matches no routing entry in the routing table, the default route in the 252 table and the service port is used for packet forwarding.

#For example, ping 10.10.50.22 without source IP.

```
admin@Xorplus$ping 10.10.50.22
PING 10.10.50.22 (10.10.50.22) 56(84) bytes of data.
From 192.168.2.1 icmp_seq=1 Destination Host Unreachable
From 192.168.2.1 icmp_seq=2 Destination Host Unreachable
^C
--- 10.10.50.22 ping statistics ---
```

```
9 packets transmitted, 0 received, +8 errors, 100% packet loss, time 8003ms
pipe 4
```

When the source address carried in a packet is the IP address of the eth0 management interface, the packet will match the IP rule: "*2000: from 10.10.51.142 lookup main*". For example, ping 10.10.50.22 with source IP 10.10.51.142.

```
admin@Xorplus$ping -I 10.10.51.142 10.10.50.22
PING 10.10.50.22 (10.10.50.22) from 10.10.51.142 : 56(84) bytes of data.
64 bytes from 10.10.50.22: icmp_req=1 ttl=63 time=0.183 ms
64 bytes from 10.10.50.22: icmp_req=2 ttl=63 time=0.153 ms
^C
--- 10.10.50.22 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 9999ms
rtt min/avg/max/mdev = 0.139/0.151/0.183/0.014 ms
```

Display System EEPROM Data Block

The system EEPROM data block information is saved in the directory: /sys/class/swmon/hwinfo/onie_syseeprom. The following example shows how to view the system EEPROM data block.

```
root@XorPlus$cat /sys/class/swmon/hwinfo/onie_syseeprom
Product Name: S4048ON
 Part Number: 099TJK
Serial Number: CN099TJK282985640054
Base MAC Address: 34:17:EB:FA:90:C4
Manufacture Date: 06/08/2015 20:36:30
Device Version: 06/08/2015 20:36:30
Label Revision: A00
Platform Name: x86_64-dell_s4000_c2338-r0
Loader Version: 3.21.1.1
MAC Addresses: 256
Manufacturer: 28298
Country Code: CN
Vendor Name: CN
Diag Version: CN
Service Tag: FX4PX42
Vendor Extension:  0x36 0x37 0x34 0x2D 0x46 0x46
```

Manual File Backup

NOTE:

Only FS S5810 Series, S3410 Series and S5860 Series switches need to do manual file backup.

FS S5810 Series, S3410 Series and S5860 Series switches use the OverlayFS file system which doesn't allow the user files on the switch to be saved from the RAM to the flash automatically. This results in the loss of user files when the switch is powered off. The user can add the file path (the file that you want to be saved even after power off) to the backup list, in */mnt/open/picos/backup_files* file, and then run the **save_config** command. With this technique, the user files on the backup list are backed up to the flash ensuring that the user files are not lost when the power is turned off.

PICOS has built-in default backup files, as listed below.

```
root@Xorplus$ cat /etc/picos/backup_files.lst
 /etc/passwd
 /etc/shadow
 /etc/group
 /etc/gshadow
 /etc/resolv.conf
 /etc/picos/picos_start.conf
 /etc/picos/switch-public.key
 /etc/picos/pica.lic
 /pica/config/pica_startup.boot
 /pica/config/pica.conf.01
 /pica/config/pica.conf.02
 /pica/config/pica.conf.03
 /pica/config/pica.conf.04
 /pica/config/pica.conf.05
 /ovs/ovs-vswitchd.conf.db
 /ovs/function.conf.db
 /ovs/config/meters
 /ovs/config/groups
 /ovs/config/flows
 /ovs/var/lib/openvswitch/pki/
 /var/log/report_diag.log
 /var/log/report_diag.log.1
 /var/log/report_diag.log.2
 /var/log/report_diag.log.3
 /var/log/report_diag.log.4
 /var/log/report_diag.log.5
/cftmp/upgrade.log
/cftmp/upgrade2.log
```

Warning:
If the user operation makes change to the above files, you need to manually run the configuration saving command to save these files from the RAM to the flash. For details, please refer to Configuration Saving Guide and copy running-config startup-config.

If you want to save a user files that are not in the above default backup file list, you can follow the backup operation steps described below.

Step1 Add the file path (the file that you want to be saved even after power off) to the backup list, in */mnt/open/picos/backup_files* file.

For example, if you want to backup **/home/admin/a.txt**, then add **/home/admin/a.txt** to the backup file list:

```
root@Xorplus$ cat /etc/picos/user_backup_files.lst
/home/admin/a.txt
```

Step2 Under Linux bash, issue the following command manually to begin file backup.

```
root@Xorplus$ save_config
```

After the above two steps, the user file **/home/admin/a.txt** will be backed up to the flash. This file will not be lost when the power is turned off.

PICOS Monitor

The PICOS Monitor process is a daemon service managed by systemd, it starts before PICOS, and is responsible for the following functions.

- **Monitor PICOS Process**

Restart PICOS if any key process crashs. If restart cannot recover the system, the system will be rebooted.

When a system failure happens, the system LED will enter the warning state.

- **Backup and Restore the Monitored Files**

Backup and restore the monitored files when the system starts up again from a power down. Monitored files are mainly the configurations that could have under updation when a power cycle happened. User application files can be protected as well.

- **Monitor CPU Usage Rate**

Generate a log message if the CPU rate is higher than maximum threshold and stays there for some time period. A log message will be recorded when the CPU usage recovers to the normal rate.

- **Monitor the Memory Usage of PICOS and User Applications**

The memory usage monitored is the physical memory used, not including any system cache of file system.

- **Monitor Disk Usage**

Monitor disk usage, including free space of rootfs, tmpfs, ramdisk and user data partition.

- **Take Care of Watchdog**

PICOS Monitor initializes and feeds the watchdog register to make sure monitor itself is alive. If monitor process fails, the watchdog will trigger to reset the whole system and load the system again.

View Monitor Log

Log messages generated during Monitor process can be found at any of the following two paths. The log entries will have the keyword **[PICOS_MONITOR]**.

```
admin@Xorplus:~$ sudo journalctl /pica/bin/system/tools/picos_monitor/monitor
-- Journal begins at Thu 2022-06-09 14:56:49 UTC, ends at Thu 2022-06-09 16:00:06 UTC. --

admin@Xorplus:~$ tail -f /tmp/log/messages
Jan 17 2022 14:17:44 57switch  local0.info : [PICA_LIB_COMMON]Card batch set port state(2) successfully.
Jan 17 2022 14:17:48 57switch ntpd daemon.info : kernel reports TIME_ERROR: 0x41: Clock Unsynchronized
Jan 17 2022 14:25:01 57switch su auth.notice : (to www-data) root on none
```

Monitor Process Management

We can use **systemctl status picos-monitor** command to check the status of monitor process, where ”Active: ” could be active or inactive, indicating the status of monitor process.

```
admin@Xorplus:~$ sudo systemctl status picos-monitor
 * picos-monitor.service - Picos Monitor
    Loaded: loaded (/lib/systemd/system/picos-monitor.service; enabled)
    Active: active (exited) since Mon 2001-01-08 18:43:02 UTC; 4h 40min ago
   Process: 648 ExecStart=/etc/init.d/picos_monitor start (code=exited, status=0/SUCCESS)
  Main PID: 648 (code=exited, status=0/SUCCESS)
    CGroup: /system.slice/picos-monitor.service
```

The following commands can be used to start/stop picos-monitor process.

```
admin@Xorplus:~$ sudo systemctl stop picos-monitor
admin@Xorplus:~$ sudo systemctl start picos-monitor
```

Enable Web-based Management Interface

> **NOTE:**
>
> When the RESTCONF is enabled, it occupies ports 80 and 443 by default. Since picos-web service also uses these default ports, it may fail to function properly. To use picos-web service on switches with RESTCONF enabled, you must configure picos-web service to use a custom port.

Overview

This feature provides control over the device's web-based management interface via HTTP/HTTPS, allowing administrators to enable or disable web access for enhanced security or preferred management style.

The command **set system services web disable <true | false>** can be used to enable or disable the web service on the system:

- Setting **true** disables the web service, blocking access to the device's web-based management interface. This is often done to enhance security by reducing access points to the system, particularly when the web interface is not needed.
- Setting **false** enables the web service, allowing access to the device's management interface via a web browser (HTTP/HTTPS). This option may be useful in environments where web-based management is the preferred method.

Disabling the web service reduces the number of access points, which is often recommended in high-security environments to minimize potential attack surfaces. In environments where CLI management (e.g., SSH) is preferred over web-based interfaces, this command helps ensure that only authorized access methods are available. This command provides administrators with flexibility in managing access to the device's web interface, helping to align with specific network security policies or management preferences.

Supported Platforms

Not all devices support this command; only platforms that support the PICOS web configuration interface can apply this configuration. For specific compatibility details, please refer to PICOS-WEB_User_Configuration_Manual .

Among the platforms supporting the PICOS web configuration interface, the default settings for web access may vary:

- **ARM models**: Web access is enabled by default.
- **X86 models**: Web access is disabled by default.

The device model (ARM or X86) can be identified using the Linux command:

```
admin@PICOS:~$ uname -m
armv7l
admin@leaf04:~$ uname -m
x86_64
```

Linux command: ssh/scp/ping/traceroute/apt-get/telnet

If management VRF is enabled, and you want to find the next-hop route in management VRF when running the commands **traceroute/SCP/ping/apt get/SSH** at Linux prompt, that is, using Eth0/1 management interface as the route interface, you have to add **ip vrf exec mgmt-vrf** before the commands.

The example format of these commands is shown below:

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> **traceroute** 10.10.51.11

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> **scp** admin@10.10.51.18:/home/Pica8.pm

sudo ip vrf exec <mgmt-vrf|*vrf-name***> ping** 10.10.51.1

sudo ip vrf exec <mgmt-vrf|*vrf-name*> **apt-get update**

sudo ip vrf exec <mgmt-vrf|*vrf-name*> **ssh** <*ip-address*>

sudo ip vrf exec <mgmt-vrf|*vrf-name*> **telnet** {<*ip-address*>|<*host-name*>} [<*port-number*>]

ip vrf exec <**mgmt-vrf|***vrf-name*> is added to specify which VRF to run the command in. If not specified, find the next hop routing information from the default VRF.

For example,

- The following command traceroutes the gateways for the host with the IP address 10.10.50.33 in default VRF.

```
admin@PICOS:~$ sudo traceroute 10.10.51.33
traceroute to 10.10.51.33 (10.10.51.33), 30 hops max, 60 byte packets
 1  10.10.51.57 (10.10.51.57)  3060.699 ms !H  3060.613 ms !H  3060.588 ms !H
```

- The following command checks whether the host at 10.10.51.1 is reachable in default VRF.

```
admin@PICOS:~$ sudo ping 10.10.51.1
PING 10.10.51.1 (10.10.51.1) 56(84) bytes of data.
64 bytes from 10.10.51.1: icmp_seq=1 ttl=64 time=1.94 ms
64 bytes from 10.10.51.1: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 10.10.51.1: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 10.10.51.1: icmp_seq=4 ttl=64 time=146 ms
64 bytes from 10.10.51.1: icmp_seq=5 ttl=64 time=2.01 ms


--- 10.10.51.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.943/30.832/146.173/57.670 ms
```

- The following command checks whether the host at 10.10.51.205 is reachable in management VRF.

```
admin@PICOS:~$ sudo ip vrf exec mgmt-vrf ping 10.10.51.205
PING 10.10.51.205 (10.10.51.205) 56(84) bytes of data.
64 bytes from 10.10.51.205: icmp_seq=1 ttl=255 time=0.746 ms
64 bytes from 10.10.51.205: icmp_seq=2 ttl=255 time=1.17 ms
64 bytes from 10.10.51.205: icmp_seq=3 ttl=255 time=1.72 ms
64 bytes from 10.10.51.205: icmp_seq=4 ttl=255 time=1.36 ms
^C
--- 10.10.51.205 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.746/1.249/1.722/0.352 ms
```

- The following command connects to 10.10.51.205 in management VRF using the default Telnet port (23).

```
admin@PICOS:~$ sudo ip vrf exec mgmt-vrf telnet 10.10.51.205
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

PICOS Open vSwitch Configuration Guide

The OpenFlow protocol is driven by ONF (Open Networking Foundation), a leader in software-defined networking (SDN). The OpenFlow protocol encompasses three essential components of an SDN framework:

1. A physical OpenFlow switch.
2. A virtual OpenFlow switch to manage virtual machines.
3. An OpenFlow controller, to organize all network pieces.

> **Warning:**
> On FS S5810 Series and S5860 Series switches, run "save_config" command when set OVS commands. Otherwise, the OVS configuration will be lost after PicOS reboot. For detail, please refer to Configuration Saving Guide.

> The Pica8 PicOS software supports features in OpenFlow 1.0 / OpenFlow 1.1 / OpenFlow1.2 / OpenFlow 1.3.x and OpenFlow 1.4. The details of feature supports in OpenFlow1.3.0 and OpenFlow 1.4.0 please see PicOS Support for OpenFlow 1.3.0 and PicOS Support for OpenFlow 1.4.0.

The following websites provide detailed information on Open vSwitch and the OpenFlow protocol.

- **Open vSwitch:** http://openvswitch.org
- **OpenFlow:** http://www.opennetworking.org/sdn-resources/openflow

PicOS can run in two different modes:

- **OVS (Open vSwitch) mode:** In this mode, PicOS is dedicated and optimized for Openflow applications.
- **L2/L3 (Layer 2/Layer 3) mode:** In this mode, PicOS can run switching and routing protocols, as well as OpenFlow applications

In OVS mode, L2/L3 daemons are not running; the system is fully dedicated to Openflow and OVS.

In L2/L3 mode, L2/L3 daemons are running, but OVS can also be activated if Crossflow Mode Introduction is activated.

This chapter assumes that the PicOS OVS mode is active. Please see PICOS Mode Selection to modify the PicOS mode.

OpenFlow Support Matrix

- PicOS Support for OpenFlow 1.4
- PicOS Support for OpenFlow 1.4.0
- PicOS Support for OpenFlow 1.3.0
- PicOS Support for OpenFlow 1.3

Introduction to Open vSwitch

Introduction to OpenFlow

OVS Web User Interface

- Login Interface
- Monitoring the Switch
- Adding a Bridge
- Add a Port
- Add GRE Port
- Add Group Table
- Add or Edit a Controller
- Edit Flow Tables
- Edit Lag Interface

Configuring Open vSwitch

- Basic Configuration in OVS Mode
- Configuring sFlow v5
- Configuring Port Mirroring
- OVSDB file
- OVS LLDP
- Enabling Radius in PicOS OVS Mode
- Inventory Database
- Broadcom Chip Limitation in OVS
- OVS CLI Enhancements
- Configuring Meter
- Configuration saving
- Configuring Buffer management
- Configuring snmp
- Configuring/Enabling SNMPv3
- Configuring Precision Time Protocol

- Configuring Tunneling
- Configuring Bridge and Ports
- Configuring LAG and LACP
- Configuring QoS
- Configuring Flow Table
- Configuring Group
- Configuring Controller or Manager
- Configuring Counter
- Switching Open vSwitch version
- Configuring rate limit
- Configuring IPv4/IPv6 address for management port
- Configuring the Duplex Mode of Optical Port
- Configuring Port Speed on AS9716-32D and N9550-32D

Examples and Topologies

- GRE Tunnel
- Multiple Virtual Bridges
- SSL Connection to Controller
- ECMP
- 802.1Q VLAN
- MPLS Network

PICOS OpenFlow Tutorials

- Basic Bridge Configuration
- Basic Flow Configurations
- Connection to a RYU Controller
- Connection to OpenDaylight Controller
- Connection to a Floodlight Controller
- Configuration Guide for Atrium Stack on ONOS Controller

Feature Supported in PicOS OVS

- Feature supported in different platform
- Match fields supported

OpenFlow Support Matrix

- PicOS Support for OpenFlow 1.3
- PicOS Support for OpenFlow 1.3.0
- PicOS Support for OpenFlow 1.4
- PicOS Support for OpenFlow 1.4.0

PicOS Support for OpenFlow 1.3

The following table contains OpenFlow 1.3 features supported by PicOS. For clarity, the feature names in this table are identical to the feature names found in OpenFlow Switch Specification Version 1.3.0.

Table 1 OpenFlow 1.3 Features Supported by PicOS

OpenFlow V1.3 Section #	Title	Features	Additional Feature Specification	R2.0OVS	R2.0XF TCAM	R2.1OVS	R2.1XF TCAM	R2.0 Limitation
1	Introduction	NA						
2	Switch Components	Flow tables		Y	Y	Y	Y	
		Group table		Y	N	Y	Y	Select & fast Fail over are not supported
3	Glossary							
4	OpenFlow Ports	See Section 4.3 - 4.5		Y	Y	Y	Y	
4.1	OpenFlow Ports	See Section 4.3 - 4.5		Y	Y	Y	Y	
4.2	Standard Ports	See Section 4.3 - 4.5		Y	Y	Y	Y	
4.3	Physical Ports	Ingress	OpenFlow packets are received on an ingress port, processed by the OpenFlow pipeline. The packet ingress port is a property of the packet throughout the OpenFlow pipeline and represents the OpenFlow port on which the packet was received into the OpenFlow switch	Y	Y	Y	Y	
		Output	The OpenFlow pipeline can decide to send the packet on an output port using the output action (see 5.9), which defines how the packets goes back to the network	Y	Y	Y	Y	
		Groups		Y	Y	Y	Y	
		Hardware interface		N	N	N	N	
		Virtual slicing of hardware interface		Y	Y	Y	Y	
4.4	Logical Ports	Logical ports are switch defined ports that don't correspond directly to a hardware interface of the switch	Logical ports are higher level abstractions that may be defined in the switch using non-OpenFlow methods					
			LAG	Y	N	Y	Y	
			Tunnels	Y	N	Y	N	
			Loopback interface	N	N	N	N	
		Ingress		Y	Y	Y	Y	
		Output		Y	Y	Y	Y	
		Groups		Y		Y	Y	
		Map to various physical port		N	N	N	N	
		PACKET_IN reports logical port and its underlying physical port (GRE & LAG)		N	N	N	N	only logical port
4.5	Local Reserved Port	Ingress		N	N	N	N	
		Output		Y	Y	Y	Y	
		Groups		Y	N	Y	Y	
		ALL	Only as an output port	Y	Y	Y	Y	
		CONTROLLER	Represent the control channel with the OpenFlow controller	Y	Y	Y	Y	
		TABLE	Represent the start of the OpenFlow pipeline	Y	Y	Y	Y	
		IN_PORT	Used only as an output port, send the packet out its ingress port	N	N	N	N	
		ANY	Cannot be used as an ingress port nor as an output port	Y	Y	Y	Y	

		LOCAL	Represent the switch's local networking stack. Can be used as an ingress port or as an output port	Y	Y	Y	Y	Linux networking stack
			The local port enables remote entities to interact with the switch via the OpenFlow network, rather than via a separate control network. it can be used to implement an in-band controller connection					
		NORMAL	Non-OpenFlow pipelineused only as an output port	N	N	N	Y	
		FLOOD	Flooding using the normal pipeline of the switch, used only as an output port	Y	Y	Y	Y	
			Packet out all standard ports	Y	Y	Y	Y	
			But not to the ingress port or ports that are in OFPPS_BLOCKED state	Y	Y	Y	Y	
5	OpenFlow Tables							
5.1	Pipeline Processing	OpenFlow-only	All packets are processed by the OpenFlow pipeline	Y	N	Y	Y	Software Implementation for ARP match/action, multiple tables
		OpenFlow-hybrid	OpenFlow operation and normal Ethernet switching operation	N	N	N	Y	
			VLAN tag to decide whether to process the packet using which pipeline	N	N	N	N	Port based since R2.0
			Input port to decide whether to process the packet using which pipeline	N	N	N	N	
			Allow a packet to go from the OpenFlow pipeline to the normal pipeline through the NORMAL and FLOOD reserved ports	N	Y	N	Y	
		Multiple flow tables		Y	N	Y	Y	Multiple flow tables are logical tables maintained by software, then mergered & installed in one physical flow table. Certain restrictions of flow rule across tables are prohibited (e.g., modify field in table 1 then matched in table 2, error should returned)
		Sequentially numbered, starting at 0.		Y	Y	Y	Y	
		Only go forward and not backward		Y	Y	Y	Y	
		Last table of the pipeline can not include the Goto instruction		Y	N	Y	Y	
		Table miss behavior configuration	Send packets to the controller	Y	Y	Y	Y	
			Drop the packet	Y	Y	Y	Y	
			The packet is processed by the next sequentially numbered table	N	N	N	N	
			The packet is processed by L2/L3 pipelines	N	N	N	N	
5.2	Flow Table	Flow table entry	Match fields	Y	Y	Y	Y	set vlans dot1q-tunneling egress t2 from customer-vlan 10
			Counters	Y	Y	Y	Y	set vlans dot1q-tunneling egress t2 from service-vlan 200
			Instructions	Y	Y	Y	Y	set vlans dot1q-tunneling egress t2 then action change
								set vlans dot1q-tunneling egress

								t2 then service-vlan 100
5.3	Matching	Packet headers		Y	Y	Y	Y	
		Ingress port		Y	Y	Y	Y	
		Metadata fields	Used to pass information between tables	N	N	N	N	
		State transition	Actions applied in a previous table using the Apply-Actions are reflected in the packet match field	N	N	N	N	
		Support ANY	Matches all possible values in the header	Y	Y	Y	Y	
		Support arbitrary bitmasks on specific match fields		Y	Y	Y	Y	
		Select highest priority flow entry		Y	Y	Y	Y	
		Counters associated with the selected flow entry must be updated		Y	Y	Y	Y	
		CHECK_OVERLAP bit on flow mod messages to avoid overlapping entries		Y	N	Y	Y	software check
		Multiple matching flow entries with the same highest priority		N	N	N	N	Chip limitation
		Support OFPC_FRAG_REASM flag	IP fragments must be reassembled before pipeline processing	N	N	N	N	
		Behavior when a switch receives a corrupted packet		N	N	N	N	
5.4	Group Table	Group identifier	A 32 bit unsigned integer	Y	N	Y	Y	
		Group type	To determine group semantics	Y	N	Y	Y	Select, indirect, fast failover group table types are not supported
		Counters	Updated when packets are processed by a group	Y	N	Y	Y	
		Action buckets	An ordered list of action buckets	Y	N	Y	Y	
5.4.1	Group Types	All	Execute all buckets in the group for multicast or broadcast	Y	N	Y	Y	
			Packet clone is dropped if a bucket directs a packet explicitly out the ingress port	Y	N	Y	Y	
			Support output action to the OFPP_IN_PORT reserved port	Y	N	Y	Y	
		Select	Execute one bucket in the group based on a switch-computed selection algorithm	N	N	Y	Y	
		Indirect	Execute the one defined bucket in this group	Y	Y	Y	Y	
		Fast failover	Execute the first live bucket which is associated with a live port/group is selected	Y	Y	Y	Y	
	ECMP		Hashing	N	N	Y	Y	Restrcicted match & actions
			Round robin	N	N	N	N	
5.5	Per Table Counters	Reference count (active entries)	32 bits	N	N	N	N	
		Packet Lookups	64 bits	N	N	N	N	
		Packet Matches	64 bits	N	N	N	N	
	Per Flow Counters	Received Packets	64 bits	N	N	N	N	
		Received Bytes	64 bits	Y	Y	Y	Y	
		Duration (seconds)	32 bits	Y	Y	Y	Y	
		Duration (nanoseconds)	32 bits	N	N	N	N	
	Per Port Counters	Received Packets	64 bits	Y	Y	Y	Y	
		Transmitted Packets	64 bits	Y	Y	Y	Y	
		Received Bytes	64 bits	Y	Y	Y	Y	

		Transmitted Bytes	64 bits	Y	Y	Y	Y	
		Receive Drops	64 bits	Y	Y	Y	Y	
		Transmit Drops	64 bits	Y	Y	Y	Y	
		Receive Errors	64 bits	Y	Y	Y	Y	
		Transmit Errors	64 bits	Y	Y	Y	Y	
		Receive Frame Alignment Errors	64 bits	Y	Y	Y	Y	
		Receive Overrun Errors	64 bits	Y	Y	Y	Y	
		Receive CRC Errors	64 bits	Y	Y	Y	Y	
		Collisions	64 bits	Y	Y	Y	Y	
	Per Queue Counters	Transmit Packets	64 bits	N	N	N	N	
		Transmit Bytes	64 bits	N	N	N	N	
		Transmit Overrun Errors	64 bits	N	N	N	N	
	Per Group Counters	Reference Count (flow entries)	32 bits	Y	Y	Y	Y	
		Packet Count	64 bits	N	N	N	N	
		Byte Count	64 bits	Y	Y	Y	Y	
	Per Bucket Counters	Packet Count	64 bits	N	N	N	N	
		Byte Count	64 bits	N	N	N	N	
5.6	Instructions	The controller can query the switch about which of the "Optional Instruction" it supports		Y	Y	Y	Y	
		Apply-Actions action(s)	Applies the specific action(s) immediately, without any change to the Action Set	Y	Y	Y	Y	All of these feature are implemented by software
		Clear-Actions	Clears all the actions in the action set immediately	N	N	N	N	
		Write-Actions action(s)	Merges the specified action(s) into the current action set	N	N	N	N	
		Write-Metadata metadata / mask	Writes the masked metadata value into the metadata field	N	N	N	N	
		Goto-Table next-table-id	Indicates the next table in the processing pipeline	Y	Y	Y	Y	
		Clear-Actions instruction is executed before the Write-Actions instruction		N	N	N	N	
		Goto-Table is executed last		Y	Y	Y	Y	
		Reject a flow entry if it is unable to execute the instructions and return an unsupported flow error		Y	Y	Y	Y	
5.7	Action Set	Action set is associated with each packet		Y	Y	Y	Y	All of these feature are implemented by software
		Set is empty by default		Y	Y	Y	Y	
		Action set is carried between flow tables		Y	Y	Y	Y	
		When the instruction set of a flow entry does not contain a Goto-Table instruction, pipeline processing stops and the actions in the action set of the packet are executed		Y	Y	Y	Y	
		Action set contains a maximum of one action of each type		Y	Y	Y	Y	
		The actions in an action set are applied in the order specified below		Y	Y	Y	Y	
		1. copy TTL inwards		N	N	N	N	
		2. pop		Y	Y	Y	Y	

		3. push		Y	Y	Y	Y	
		4. copy TTL outwards		N	N	N	N	
		5. decrement TTL		N	N	N	N	
		6. set		Y	Y	Y	Y	
		7. qos		Y	N	Y	N	
		8. group	If a group action is specified, apply the actions of the relevant group bucket(s) in the order specified by this list.	Y	N	Y	Y	
		9. output	If no group action is specified, forward the packet on the port specified by the output action. The output action in the action set is executed last.	Y	Y	Y	Y	
			If both an output action and a group action are specified in an action set, the output action is ignored and the group action takes precedence.	Y	Y	Y	Y	
			If no output action and no group action were specified in an action set, the packet is dropped.	Y	Y	Y	Y	
			The execution of groups is recursive if the switch supports it; a group bucket may specify another group, in which case the execution of actions traverses all the groups specified by the group configuration.	Y	Y	Y	Y	
5.8	Action List	Apply-Actions instruction and the Packet-out message include an action list	The actions of an action list are executed in the order specified by the list, and are applied immediately to the packet.	Y	Y	Y	Y	
			The effect of those actions is cumulative.	Y	Y	Y	Y	
			If the action list contains an output action, a copy of the packet is forwarded in its current state to the desired port.	Y	Y	Y	Y	
			If the list contains a group actions, a copy of the packet in its current state is processed by the relevant group buckets.	N	N	Y	Y	
5.9	Actions	The controller can also query the switch about which of the "Optional Action" it supports		Y	Y	Y	Y	
		Output	Support forwarding to physical ports, switch-defined logical ports and the required reserved ports.	Y	Y	Y	Y	
		Set-Queue	The set-queue action sets the queue ID for a packet and is used to provide basic Quality-of-Service (QoS) support.	Y	Y	Y	Y	
		Drop		Y	Y	Y	Y	
		Group		Y	Y	Y	Y	
		Push-Tag/Pop-Tag	Order of header fields - Ethernet, VLAN, MPLS, ARP/IP, TCP/UDP/SCTP (IP-only).	Y	Y	Y	Y	
		Push VLAN header	Push a new VLAN header onto the packet. The Ethertype is used as the Ethertype for the tag. Only Ethertype 0x8100 and 0x88a8 should be used.	N	N	Y	N	VCAP implementation, VLAN only actions allowed
		Pop VLAN header	Pop the outer-most VLAN header from the packet.	N	N	Y	N	
		Push MPLS header	Push a new MPLS shim header onto the packet. Only Ethertype 0x8847 and 0x8848 should be used.	Y	Y	Y	Y	
		Pop MPLS header	Pop the outer-most MPLS tag or shim header from the packet.	Y	Y	Y	Y	
		Set-Field						
		Set VLAN ID		Y	Y	Y	Y	
		Strip VLAN ID		N	N	Y	N	Use reserved VLAN ID 4095 as special VLAN for stripping, 2 VLAN tags are supported

		Change-TTL	Modify the values of the IPv4 TTL, IPv6 Hop Limit or MPLS TTL in the packet.	N	N	N	N	
			If it is supported, applied to the outermost-possible header.	N	N	N	N	
		Set MPLS TTL	8 bits: New MPLS TTL, Replace the existing MPLS TTL. Only applies to packets with an existing MPLS shim header.	Y	Y	Y	Y	
		Decrement MPLS TTL	Decrement the MPLS TTL. Only applies to packets withan existing MPLS shim header.	Y	Y	Y	Y	
		Set IP TTL	Replace the existing IPv4 TTL or IPv6 Hop Limit and update the IP checksum. Only applies to IPv4 and IPv6 packets.	N	N	N	N	
		Decrement IP TTL	Decrement the IPv4 TTL or IPv6 Hop Limit field and update the IP checksum. Only applies to IPv4 and IPv6 packets.	N	N	N	N	
		Copy TTL outwards	Copy the TTL from next-to-outermost to outermost header with TTL. Copy can be IP-to-IP, MPLS-to-MPLS, or IP-to-MPLS.	N	N	N	N	
		Copy TTL inwards	Copy the TTL from outermost to next-to-outermost header with TTL. Copy can be IP-to-IP, MPLS-to-MPLS, or MPLS-to-IP.	N	N	N	N	
5.9.1	Default Values (for Fields on Push	Field values for all fields specified in Table 6 should be copied from existing outer headers to new outer headers	VLAN ID ← VLAN ID	Y	Y	Y	N	
		New fields listed in Table 6 without corresponding existing fields should be set to zero	VLAN priority ← VLAN priority	Y	Y	Y	N	
		Fields in new headers may be overridden by specifying a "set" action for the appropriate field(s) after the push operation	MPLS label ← MPLS label	Y	N	Y	N	
			MPLS traffic class ← MPLS traffic class	N	N	N	N	
			MPLS TTL ← MPLS TTL & IP TTL	N	N	N	N	
6	OpenFlow Channel	Encrypted using TLS		Y	Y	Y	Y	
		Directly over TCP		Y	Y	Y	Y	
6.1	OpenFlow Protocol Overview	Controller-to-switch message type	Initiated by the controller and used to directly manage or inspect the state of the switch.	Y	Y	Y	Y	
		Asynchronous message type	Initiated by the switch and used to update the controller of network events and changes to the switch state.	Y	Y	Y	Y	
		Symmetric message type	Initiated by either the switch or the controller and sent without solicitation.	Y	Y	Y	Y	
6.1.1	Controller-to-Switch	Features	Request the capabilities of a switch; the switch must respond with a features reply.	Y	Y	Y	Y	
		Configuration	Set and query configuration parameters in the switch; switch only responds to a query from the controller.	Y	Y	Y	Y	
		Modify-State	Add, delete and modify flow/group entries in the OpenFlow tables and to set switch port properties.	Y	Y	Y	Y	
		Read-State	Used by the controller to collect statistics from the switch.	Y	Y	Y	Y	
		Packet-out	Used by the controller to send packets out of a specified port on the switch, and to forward packets received via Packet-in messages.	Y	Y	Y	Y	
		Barrier	Barrier request/reply messages are used by the controller to ensure message dependencies have been met or to receive notifications for completed operations.	Y	Y	Y	Y	

6.1.2	Asynchronous	Switches send asynchronous messages to controllers to denote a packet arrival, switch state change, or error						
		Packet-in	For all packets that do not have a matching flow entry, the if table configuration is configured for packets forwarded to the CONTROLLER reserved port, a packet-in event is always sent to controllers.	Y	Y	Y	Y	
			If the packet-in event is configured to buffer packets then the packet-in events contain some fraction of the packet header and a buffer ID to be used by a controller when it is ready for the switch to forward the packet.	Y	Y	Y	Y	
			If the packet is buffered, the number of bytes of the original packet to include in the packet-in can be configured. By default, it is 128 bytes.	Y	Y	Y	Y	
			Or table miss it can be configured in the switch configuration.	Y	Y	Y	Y	
			For packet forwarded to the controller it can be configured in the output action.	Y	Y	Y	Y	
		Flow-Removed	Only sent for flow with the OFPFF_SEND_FLOW_REM flag set.	Y	Y	Y	Y	
			Generated as the result of a controller flow delete requests or the switch flow expiry process when one of the flow timeout is exceeded.	Y	Y	Y	Y	
		Port-status	Send port-status messages to controllers as port configuration or port state changes.	Y	Y	Y	Y	
		Error	Notify controllers of problems using error messages.	Y	Y	Y	Y	
6.1.3	Symmetric	Sent without solicitation, in either direction						
		Hello	Exchanged between the switch and controller upon connection startup.	Y	Y	Y	Y	
		Echo	Sent from either the switch or the controller, and must return an echo reply.	Y	Y	Y	Y	
		Experimenter	A standard way for OpenFlow switches to offer additional functionality within the OpenFlow message type space.	Y	Y	Y	Y	
6.2	Connection Setup	Establish communication with a controller at a user-configurable (but otherwise fixed) IP address, using a user-specified port	Traffic to and from the OpenFlow channel is not run through the OpenFlow pipeline. Therefore, the switch must identify incoming traffic as local before checking it against the flow tables.	Y	Y	Y	Y	
			Each side of the connection must immediately send an OFPT_HELLO message with the version field set to the highest OpenFlow protocol version supported by the sender.	Y	Y	Y	Y	
			The recipient may calculate the OpenFlow protocol version to be used as the smaller of the version number that it sent and the one that it received.	Y	Y	Y	Y	
			If the negotiated version is not supported by the recipient, the recipient must reply with an OFPT_ERROR message with a type field of OFPET_HELLO_FAILED, a code field of OFPHFC_COMPATIBLE, and then terminate the connection.	Y	Y	Y	Y	
			Optionally an ASCII string explaining the situation in data.	Y	Y	Y	Y	
6.3	Multiple Controllers	Establish communication withmultiple controllers	Controller fail-over.	Y	Y	Y	Y	Active & Standby controllers
			Controller load balancing.	N	N	N	N	
			Switch virtualisation.	Y	Y	Y	Y	
			Switch must connect to all controllers it is configured with, and try to maintain connection with all of them concurrently.	Y	Y	Y	Y	
			The reply or error messages related to those command must only be sent on the controller	Y	Y	Y	Y	

			connection associated with that command.					
			Asynchronous messages may need to be send to multiple controllers, the message is duplicated for each eligible controller connection and each message sent when the respective controller connection allows it.	Y	Y	Y	Y	
		The default role of a controller is OFPCR_ROLE_EQUAL	Controller has full access to the switch and is equal to other controllers in the same role.	Y	Y	Y	Y	
			Controller receives all the switch asynchronous messages (such as packet-in, flow-removed).	Y	Y	Y	Y	
			The controller can send controller-to-switch commands to modify the state of the switch.	Y	Y	Y	Y	
			The switch does not do any arbitration or resource sharing between controllers.	Y	Y	Y	Y	
		Controller can request its role to be changed to OFPCR_ROLE_SLAVE	Controller has read-only access to the switch.	Y	Y	Y	Y	
			Controller does not receive switch asynchronous messages, apart from Port-status messages.	Y	Y	Y	Y	
			The controller is denied ability to send controller-to-switch commands that modify the state of the switch, OFPT_PACKET_OUT, OFPT_FLOW_MOD, OFPT_GROUP_MOD, OFPT_PORT_MODand OFPT_TABLE_MOD.	Y	Y	Y	Y	
			If the controller sends one of those commands, the switch must reply with an OFPT_ERROR message with a type field of OFPET_BAD_REQUEST, a code field of OFPBRC_IS_SLAVE.	Y	Y	Y	Y	
			Othercontroller-to-switch messages, such as OFPT_STATS_REQUEST and OFPT_ROLE_REQUEST, should be processed normally.	Y	Y	Y	Y	
		A controller can request its role to be changed to OFPCR_ROLE_MASTER	The switch makes sure there is only a single controller in this role.	Y	Y	Y	Y	
			When a controller change its role to OFPCR_ROLE_MASTER, the switch change all other controllers which role is OFPCR_ROLE_MASTER to have the role OFPCR_ROLE_SLAVE.	Y	Y	Y	Y	
			When the switch perform such role change, no message is generated to the controller which role is changed (in most case that controller is no longer reachable).	Y	Y	Y	Y	
		A switch may be simultaneously connected to multiple controllers in Equal state, multiple controllers in Slave state, and at most one controller in Master state	Each controller may communicate its role to the switch via a OFPT_ROLE_REQUEST message, and the switch must remember the role of each controller connection. A controller may change role at any time.	Y	Y	Y	Y	
			To detect out-of-order messages during a master/slave transition, the OFPT_ROLE_REQUEST message contains a 64-bit sequence number field, generation_id, that identifies a given mastership view.	Y	Y	Y	Y	
		On receiving a OFPT_ROLE_REQUEST with role equal to OFPCR_ROLE_MASTER or OFPCR_ROLE_SLAVEthe switch must compare the generation_id in the message against the largest generation id seen sofar	A message with a generation_id smaller than a previously seen generation id must be considered stale and discarded. The switch must respond to stale messages with an error message with typeOFPET_ROLE_REQUEST_FAILED and code OFPRRFC_STALE.	Y	Y	Y	Y	
6.4	Connection Interruption	A switch loses contact with all controllers, the switch should immediately enter either "fail secure mode" or "fail standalone mode"	In "fail secure mode", the only change to switch behavior is that packets and messages destined to the controllers are dropped.	Y	Y	Y	Y	
			Flows should continue to expire according to their timeouts in "fail secure mode."	Y	Y	Y	Y	
			In "fail standalone mode," the switch processes all packets using the OFPP_NORMAL port; in other words, the switch acts as a legacy Ethernet switch or router.	Y	Y	Y	Y	
			Upon connecting to a controller again, the existing flow entries remain.	Y	Y	Y	Y	

			The controller then has the option of deleting all flow entries, if desired.	Y	Y	Y	Y	
		The first time a switch starts up, it will operate in either "fail secure mode" or "fail standalone mode" mode, until is successfully connects to a controller		Y	Y	Y	Y	
6.5	Encryption	The switch and controller may communicate through a TLS connection	The TLS connection is initiated by the switch on startup to the controller, which is located by default on TCP port 6633	Y	Y	Y	Y	
			Each switch must be user-configurable with one certificate for authenticating the controller (controller certificate) and the other for authenticating to the controller (switch certificate)	Y	Y	Y	Y	
6.6	Message Handling	Message Delivery	Messages are guaranteed delivery, unless the connection fails entirely.	Y	Y	Y	Y	
		Message Processing	Switches must process every message received from a controller in full, possibly generating a reply.	Y	Y	Y	Y	
			If a switch cannot completely process a message received from a controller, it must send back an error message.	Y	Y	Y	Y	
			Switches must send to the controller all asynchronous messages generated by internal state changes, such as flow-removed or packet-in messages.	Y	Y	Y	Y	
	Message Ordering	Ordering can be ensured through the use of barrier messages	In the absence of barrier messages, switches may arbitrarily reorder messages to maximize performance.	N	N	N	N	
			Messages must not be reordered across a barrier message and the barrier message must be processed only when all prior messages have been processed.	Y	Y	Y	Y	
			Messages before a barrier must be fully processed before the barrier, including sending any resulting replies or errors.	Y	Y	Y	Y	
			The barrier must then be processed and a barrier reply sent.	Y	Y	Y	Y	
			Messages after the barrier may then begin processing.	Y	Y	Y	Y	
6.7	Flow Table Modification Messages	OFPFC_ADD	For add requests (OFPFC_ADD) with the OFPFF_CHECK_OVERLAP flag set, the switch must first check for any overlapping flow entries in the requested table	Y	Y	Y	Y	
			If an overlap conflict exists between an existing flow entry and the add request, the switch must refuse the addition and respond with an ofp_error_msg with OFPET_FLOW_MOD_FAILED type and OFPFMFC_OVERLAP code	Y	Y	Y	Y	
			If a flow entry with identical match fields and priority already resides in the requested table, then that entry, including its duration, must be cleared from the table, and the newflow entry added	Y	Y	Y	Y	
			If the OFPFF_RESET_COUNTS flag is set, the flow entry counters must be cleared, otherwise they should be copied from the replaced flow	N	N	N	N	
			No flow-removed message is generated for the flow entry eliminated as part of an add request; if the controller wants a flow-removed message it should explicitly send a DELETE STRICT for the old flow prior to adding the new one	Y	Y	Y	Y	
			If a switch cannot find any space in the requested table in which to add the incoming flow entry, the switch should send an ofp_error_msg with OFPET_FLOW_MOD_FAILED type and OFPFMFC_TABLE_FULL code.	N	N	N	N	
		OFPFC_MODIFY or OFPFC_MODIFY_STRICT	If a matching entry exists in the table, the instructions field of this entry is updated with the value from the request, whereas its cookie, idle_timeout, hard_timeout, flags, counters and duration fields are left unchanged.	Y	Y	Y	Y	

			If the OFPFF_RESET_COUNTS flag is set, the flow entry counters must be cleared.	N	N	N	N	
			If no flow currently residing in the requested table matches the request, no error is recorded, and no flow table modification occurs.	Y	Y	Y	Y	
			In the strict versions, the set of match fields, all match fields, including their masks, and the priority, are strictly matched against the entry, and only an identical flow is modified or removed.	Y	Y	Y	Y	
			If the match in a flow mod specifies an arbitrary bitmask for another field which the switch cannot support, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and OFPBMC_BAD_MASK code.	Y	Y	Y	Y	
			If the match in a flow mod specifies values that cannot be matched, for example, a VLAN ID greater than 4095 and not one of the reserved values, or a DSCP value with one of the two higher bits set, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and OFPBMC_BAD_VALUE code.	Y	Y	Y	Y	
			If the match in a flow mod message specifies a field that is unsupported in the table, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and OFPBMC_BAD_FIELD code.	Y	Y	Y	Y	
			If the match in a flow mod message specifies a field more than once, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and OFPBMC_DUP_FIELD code.	Y	Y	Y	Y	
			If the match in a flow mod message specifies a field but fail to specify its associated prerequisites, for example specifies an IPv4 address without matching the EtherType to 0x800, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and OFPBMC_BAD_PREREQ code.	Y	Y	Y	Y	
			If the match in a flow mod specifies an arbitrary bitmask for either the datalink or network addresses which the switch cannot support, the switch must return an ofp_error_msg with OFPET_BAD_MATCH type and either OFPBMC_BAD_DL_ADDR_MASK or OFPBMC_BAD_NW_ADDR_MASK.	Y	Y	Y	Y	
			If an action in a flow mod message references a group that is not currently defined on the switch, or is a reserved group, such as OFPG_ALL, the switch must return an ofp_error_msg with OFPET_BAD_ACTION type and OFPBAC_BAD_OUT_GROUP code.	Y	Y	Y	Y	
			If an action in a flow mod message has a value that is invalid, for example a Set VLAN ID action with value greater than 4095, or a Push action with an invalid Ethertype, the switch should return an ofp_error_msg with OFPET_BAD_ACTION type and OFPBAC_BAD_ARGUMENT code.	Y	Y	Y	Y	
			If an action in a flow mod message performs an operation which is inconsistent with the match, for example, a pop VLAN action with a match specifying no VLAN, or a set IPv4 address action with a match wildcarding the Ethertype, the switch may optionally reject the flow and immediately return an ofp_error_msg with OFPET_BAD_ACTION type and OFPBAC_MATCH_INCONSISTENT code.	Y	Y	Y	Y	
			If any other errors occur during the processing of the flow mod message, the switch may return an ofp_error_msg with OFPET_FLOW_MOD_FAILED type and OFPFMC_UNKNOWN code.	Y	Y	Y	Y	
		OFPFC_DELETE or OFPFC_DELETE_STRICT	If a matching entry exists in the table, it must be deleted.	Y	Y	Y	Y	
			If the entry has the OFPFF_SEND_FLOW_REM flag set, it should generate a flow removed message.	Y	Y	Y	Y	
			If no flow currently residing in the requested table matches the request, no error is recorded, and no flow table modification occurs.	Y	Y	Y	Y	

			In the strict versions, the set of match fields, all match fields, including their masks, and the priority, are strictly matched against the entry, and only an identical flow is modified or removed.	Y	Y	Y	Y	
			For non-strict modify and delete commands, all flows that match the flow mod description are modified or removed.	Y	Y	Y	Y	
			In the non-strict versions, a match will occur when a flow entry exactly matches or is more specific than the description in the flow mod command; in the flow mod the missing match fields are wildcarded, field masks are active, and other flow mod fields such as priority are ignored.	Y	Y	Y	Y	
			Delete commands can be optionally filtered by destination group or output port.	N	N	N	N	
			If the out_port field contains a value other than OFPP_ANY, it introduces a constraint when matching.	Y	Y	Y	Y	
			Modify and delete commands can also be filtered by cookie value.	Y	Y	Y	Y	
			Delete commands can use the OFPTT_ALL value for table-id to indicate that matching flows are to be deleted from all flow tables.	Y	Y	Y	Y	
			If the flow modification message specifies an invalid table-id, the switch should send an ofp_error_msg with OFPET_FLOW_MOD_FAILED type and OFPFMFC_BAD_TABLE_ID code.	Y	Y	Y	Y	
			If the instructions requested in a flow mod message are unknown the switch must return an ofp_error_msg with OFPET_BAD_INSTRUCTION type and OFPBIC_UNKNOWN_INST code.	Y	Y	Y	Y	
			If the instructions requested in a flow mod message are unsupported the switch must return an ofp_error_msg with OFPET_BAD_INSTRUCTION type and OFPBIC_UNSUP_INST code.	Y	Y	Y	Y	
			If the instructions requested contain a Goto-Table and the next-table-id refers to an invalid table the switch must return an ofp_error_msg with OFPET_BAD_INSTRUCTION type and OFPBIC_BAD_TABLE_ID code.	Y	Y	Y	Y	
			If the instructions requested contain a Write-Metadata and the metadata value or metadata mask value is unsupported then the switch must return an ofp_error_msg with OFPET_BAD_INSTRUCTION type and OFPBIC_UNSUP_METADATA or OFPBIC_UNSUP_METADATA_MASK code.	Y	Y	Y	Y	
			If the bitmasks specified in both the datalink and network addresses are not supported then OFPBMC_BAD_DL_ADDR_MASK should be used.	Y	Y	Y	Y	
			If any action references a port that will never be valid on a switch, the switch must return an ofp_error_msg with OFPET_BAD_ACTION type and OFPBAC_BAD_OUT_PORT code.	Y	Y	Y	Y	
			If the referenced port may be valid in the future, e.g. when a linecard is added to a chassis switch, or a port is dynamically added to a software switch, the switch may either silently drop packets sent to the referenced port, or immediately return an OFPBAC_BAD_OUT_PORT error and refuse the flow mod.	Y	Y	Y	Y	
			If an action list contain a sequence of actions that the switch can not support in the specified order, the switch should return an ofp_error_msg with OFPET_BAD_ACTION type and OFPBAC_UNSUPPORTED_ORDER code.	Y	Y	Y	Y	
6.8	Flow Removal	Switch flow expiry mechanism	Is run by the switch independently of the controller and is based on the state and configuration of flow entries.	Y	Y	Y	Y	
			A non-zero hard_timeout field causes the flow entry to be removed after the given number of	Y	Y	Y	Y	

			seconds, regardless of how many packets it has matched.					
			A non-zero idle_timeout field causes the flow entry to be removed when it has matched no packets in the givennumber of seconds.	Y	Y	Y	Y	
			The switch must implement flow expiry and remove flow entries from the flow table when one of their timeout is exceeded.	Y	Y	Y	Y	
			When a flow entry is removed, the switch must check the flow entry's OFPFF_SEND_FLOW_REM flag. If this flag is set, the switch must send a flow removed message to the controller.	Y	Y	Y	Y	
			Each flow removed message contains a complete description of the flow entry, the reason for removal (expiry or delete), the flow entry duration at the time of removal, and the flow statistics at time of removal.	Y	Y	Y	Y	
6.9	Group Table Modification Messages	OFPGC_ADD	Groups may consist of zero or more buckets.	Y	Y	Y	Y	
			A group may also include buckets which themselves forward to other groups if the switch supports it.	Y	Y	Y	Y	
			The action set for each bucket must be validated using the same rules as those for flow mods (Section 6.7), with additional group-specific checks.	Y	Y	Y	Y	
			If an action in one of the buckets is invalid or unsupported, the switch should return an ofp_error_msg with OFPET_BAD_ACTION type and code corresponding to the error.	Y	Y	Y	Y	
			If a group entry with the specified group identifier already resides in the group table, then the switch must refuse to add the group entry and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_GROUP_EXISTS code.	Y	Y	Y	Y	
			If a specified group type is invalid then the switch must refuse to add the group entry and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_INVALID_GROUP code.	Y	Y	Y	Y	
			If a switch does not support unequal load sharing with select groups (buckets with weight different than 1), it must refuse to add the group entry and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_WEIGHT_UNSUPPORTED code.	Y	Y	Y	Y	
			If a switch cannot add the incoming group entry due to lack of space, the switch must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_OUT_OF_GROUPS code.	Y	Y	Y	Y	
			If a switch cannot add the incoming group entry due to restrictions (hardware or otherwise) limiting the number of group buckets, it must refuse to add the group entry and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_OUT_OF_BUCKETS code.	Y	Y	Y	Y	
			If a switch cannot add the incoming group because it does not support the proposed liveliness configuration, the switch must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_WATCH_UNSUPPORTED code.	N	N	N	N	
		OFPGC_MODIFY	if a group entry with the specified group identifier already resides in the group table, then that entry, including its type and action buckets, must be removed, and the new group entry added.	Y	Y	Y	Y	
			If a group entry with the specified group identifier does not already exist then the switch must refuse the group mod and send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_UNKNOWN_GROUP code	Y	Y	Y	Y	
		OFPGC_DELETE	If no group entry with the specified group identifier currentlyexists in the group table, no error is	Y	Y	Y	Y	

			recorded, and no group table modification occurs					
			To delete all groups with a single message, specify OFPG_ALL as the group value	Y	Y	Y	Y	
		Groups	Groups may be chained if the switch supports it, when at least one group forward to another group, or in more complex configuration	Y	Y	Y	Y	
			If a switch does not support groups of groups, it must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_CHAINING_UNSUPPORTED code.	Y	Y	Y	Y	
			A switch may support checking that no loop is created while chaining groups.	Y	Y	Y	Y	
			If a group mod is sent such that a forwarding loop would be created, the switch must reject the group mod and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_LOOP code.	Y	Y	Y	Y	
			A switch may support checking that groups forwarded to by other groups are not removed.	N	N	N	N	
			If a switch cannot delete a group because it is referenced by another group, it must refuse to delete the group entry and must send an ofp_error_msg with OFPET_GROUP_MOD_FAILED type and OFPGMFC_CHAINED_GROUP code.	Y	Y	Y	Y	
A	Appendix A The OpenFlow Protocol							
A.2.1	Port Structures	Port_no field uniquely identifies a port within a switch	Ports are numbered starting from 1.	Y	Y	Y	Y	
		Name field is a null-terminated string containing a human-readable name for the interface		Y	Y	Y	Y	
		Port administrative settings support the following states	The OFPPC_PORT_DOWN bit indicates that the port has been administratively brought down and should not be used by OpenFlow.	Y	Y	Y	Y	
			The OFPPC_NO_RECV bit indicates that packets received on that port shouldbe ignored.	Y	Y	Y	Y	
			The OFPPC_NO_FWD bit indicates that OpenFlow should not send packets to that port.	Y	Y	Y	Y	
			The OFPPC_NO_FWD bit indicates that OpenFlow should not send packets to that port.	Y	Y	Y	Y	
			The OFPPFL_NO_PACKET_IN bit indicates that packets on that port that generate a table miss should never trigger a packet-in message to the controller	Y	Y	Y	Y	
			The port config bits are set by the controller and not changed by the switch.					
			If the port config bits are changed by the switch through another administrative interface, the switch sends an OFPT_PORT_STATUS message to notify the controller of the change.	Y	Y	Y	Y	
		State field describes the port internal state that supports the following states	OFPPS_LINK_DOWN bit indicates the physical link is not present.	Y	Y	Y	Y	
			The OFPPS_BLOCKED bit indicates that a switch protocol outside of OpenFlow, such as 802.1D Spanning Tree, is preventing the use of that port with OFPP_FLOOD.	Y	Y	Y	Y	
			OFPPS_LIVE indicates Live for Fast Failover Group.	N	N	N	N	
			All port state bits are read-only and cannot be changed by the controller.	Y	Y	Y	Y	
			When the port flags are changed, the switch sends an OFPT_PORT_STATUS message to notify the controller of the change.	Y	Y	Y	Y	
		Curr, advertised, supported, and peer fields indicate link modes (speed and duplexity), link type (copper/fiber) and link features (auto negotiation and pause)		Y	Y	Y	Y	

		Curr_speed and max_speed fields indicate the current and maximum bit rate (raw transmission speed) of the link in kbps		Y	Y	Y	Y	
A.2.2	Queue Structures	QoS (DSCP & Q mapping?)	An OpenFlow switch provides limited Quality-of-Service support (QoS) through a simple queuing mechanism. One (or more) queues can attach to a port and be used to map flows on it. Flows mapped to a specific queue will be treated according to that queue's configuration.	Y	Y	Y	Y	
A.2.3	Flow Match Structures	OpenFlow match is composed of a flow match header and a sequence of zero or more flow match fields	The only valid match type in this specification is OFPMT_OXM, the OpenFlow 1.1 match type OFPMT_STANDARD is deprecated.	Y	Y	Y	Y	
			The flow match fields are described using the OpenFlow Extensible Match (OXM) format.	Y	Y	Y	Y	
		OpenFlow specification distinguishes two types of OXM match classes	ONF member classes.					
			ONF reserved classes.					
		Flow Match Fields						
		OXM_OF_IN_PORT	/* Switch input port. */	Y	Y	Y	Y	
		OXM_OF_IN_PHY_PORT	/* Switch physical input port. */	Y	Y	Y	Y	
		OXM_OF_METADATA	/* Metadata passed between tables. */	N	N	N	N	
		OXM_OF_ETH_DST	/* Ethernet destination address. */	Y	Y	Y	Y	
		OXM_OF_ETH_SRC	/* Ethernet source address. */	Y	Y	Y	Y	
		OXM_OF_ETH_TYPE	/* Ethernet frame type. */	Y	Y	Y	Y	
		OXM_OF_VLAN_VID	/* VLAN id. */	Y	Y	Y	Y	
		OXM_OF_VLAN_PCP	/* VLAN priority. */	Y	Y	Y	Y	
		OXM_OF_IP_DSCP	/* IP DSCP (6 bits in ToS field). */	Y	Y	Y	Y	
		OXM_OF_IP_ECN	/* IP ECN (2 bits in ToS field). */	N	N	N	N	
		OXM_OF_IP_PROTO	/* IP protocol. */	Y	Y	Y	Y	
		OXM_OF_IPV4_SRC	/* IPv4 source address. */	Y	Y	Y	Y	
		OXM_OF_IPV4_DST	/* IPv4 destination address. */	Y	Y	Y	Y	
		OXM_OF_TCP_SRC	/* TCP source port. */	Y	Y	Y	Y	
		OXM_OF_TCP_DST	/* TCP destination port. */	Y	Y	Y	Y	
		OXM_OF_UDP_SRC	/* UDP source port. */	Y	Y	Y	Y	
		OXM_OF_UDP_DST	/* UDP destination port. */	Y	Y	Y	Y	
		OXM_OF_SCTP_SRC	/* SCTP source port. */	N	N	N	N	
		OXM_OF_SCTP_DST	/* SCTP destination port. */	N	N	N	N	
		OXM_OF_ICMPV4_TYPE	/* ICMP type. */	N	N	N	N	
		OXM_OF_ICMPV4_CODE	/* ICMP code. */	N	N	N	N	
		OXM_OF_ARP_OP	/* ARP opcode. */	Y	Y	Y	N	All ARP matches are supported via software
		OXM_OF_ARP_SPA	/* ARP source IPv4 address. */	Y	Y	Y	N	
		OXM_OF_ARP_TPA	/* ARP target IPv4 address. */	Y	Y	Y	N	
		OXM_OF_ARP_SHA	/* ARP source hardware address. */	Y	Y	Y	N	
		OXM_OF_ARP_THA	/* ARP target hardware address. */	Y	Y	Y	N	
		OXM_OF_IPV6_SRC	/* IPv6 source address. */	Y	Y	Y	Y	
		OXM_OF_IPV6_DST	/* IPv6 destination address. */	Y	Y	Y	Y	
		OXM_OF_IPV6_FLABEL	/* IPv6 Flow Label */	N	N	N	N	
		OXM_OF_ICMPV6_TYPE	/* ICMPv6 type. */	N	N	N	N	
		OXM_OF_ICMPV6_CODE	/* ICMPv6 code. */	N	N	N	N	
		OXM_OF_IPV6_ND_TARGET	/* Target address for ND. */	N	N	N	N	

		OXM_OF_IPV6_ND_SLL	/* Source link-layer for ND. */	N	N	N	N	
		OXM_OF_IPV6_ND_TLL	/* Target link-layer for ND. */	N	N	N	N	
		OXM_OF_MPLS_LABEL	/* MPLS label. */	Y	Y	Y	Y	
		OXM_OF_MPLS_TC	/* MPLS TC. */	N	N	N	N	
		Required match fields						
		OXM_OF_IN_PORT	Ingress port. This may be a physical or switch-defined logical port.	Y	Y	Y	Y	
		OXM_OF_ETH_DST	Ethernet source address. Can use arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_ETH_SRC	Ethernet destination address. Can use arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_ETH_TYPE	Ethernet type of the OpenFlow packet payload, after VLAN tags.	Y	Y	Y	Y	
		OXM_OF_IP_PROTO	IPv4 or IPv6 protocol number.	Y	Y	Y	Y	
		OXM_OF_IPV4_SRC	IPv4 source address. Can use subnet mask or arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_IPV4_DST	IPv4 destination address. Can use subnet mask or arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_IPV6_SRC	IPv6 source address. Can use subnet mask or arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_IPV6_DST	IPv6 destination address. Can use subnet mask or arbitrary bitmask.	Y	Y	Y	Y	
		OXM_OF_TCP_SRC	TCP source port.	Y	Y	Y	Y	
		OXM_OF_TCP_DST	TCP destination port.	Y	Y	Y	Y	
		OXM_OF_UDP_SRC	UDP source port.	Y	Y	Y	Y	
		OXM_OF_UDP_DST	UDP destination port.	Y	Y	Y	Y	
A.2.4	Flow Instruction Structures	See Section 5.6						
A.2.5	Action Structures	A number of actions may be associated with flows, groups or packets. The currently defined action types are						
		OFPAT_OUTPUT = 0,	/* Output to switch port. */	Y	Y	Y	Y	
		OFPAT_COPY_TTL_OUT = 11,	/* Copy TTL "outwards" – from next-to-outermost to outermost */	N	N	N	N	
		OFPAT_COPY_TTL_IN = 12,	/* Copy TTL "inwards" – from outermost to next-to-outermost */	N	N	N	N	
		OFPAT_SET_MPLS_TTL = 15,	/* MPLS TTL */	Y	Y	Y	Y	
		OFPAT_DEC_MPLS_TTL = 16,	/* Decrement MPLS TTL */	Y	Y	Y	Y	
		OFPAT_PUSH_VLAN = 17,	/* Push a new VLAN tag */	N	N	Y	N	
		OFPAT_POP_VLAN = 18,	/* Pop the outer VLAN tag */	N	N	Y	N	
		OFPAT_PUSH_MPLS = 19,	/* Push a new MPLS tag */	Y	Y	Y	Y	
		OFPAT_POP_MPLS = 20,	/* Pop the outer MPLS tag */	Y	Y	Y	Y	
		OFPAT_SET_QUEUE = 21,	/* Set queue id when outputting to a port */	Y	Y	Y	Y	
		OFPAT_GROUP = 22,	/* Apply group. */	Y	Y	Y	Y	
		OFPAT_SET_NW_TTL = 23,	/* IP TTL. */	N	N	N	N	
		OFPAT_DEC_NW_TTL = 24,	/* Decrement IP TTL. */	N	N	N	N	
		OFPAT_SET_FIELD = 25,	/* Set a header field using OXM TLV format. */	Y	Y	Y	Y	
		OFPAT_EXPERIMENTER = 0xffff		Y	Y	Y	Y	
		The type of a set-field action can be any valid OXM header type	OXM types OFPXMT_OFB_IN_PORT and OFPXMT_OFB_METADATA are not supported, because those are not header fields.					

		OXM_OF_IN_PHY_PORT	/* Switch physical input port. */	N	N	N	N	
		OXM_OF_ETH_DST	/* Ethernet destination address. */	Y	Y	Y	Y	
		OXM_OF_ETH_SRC	/* Ethernet source address. */	Y	Y	Y	Y	
		OXM_OF_ETH_TYPE	/* Ethernet frame type. */	Y	Y	Y	Y	
		OXM_OF_VLAN_VID	/* VLAN id. */	Y	Y	Y	Y	
		OXM_OF_VLAN_PCP	/* VLAN priority. */	Y	Y	Y	Y	
		OXM_OF_IP_DSCP	/* IP DSCP (6 bits in ToS field). */	Y	Y	Y	Y	
		OXM_OF_IP_ECN	/* IP ECN (2 bits in ToS field). */	N	N	N	N	
		OXM_OF_IP_PROTO	/* IP protocol. */	N	N	N	N	
		OXM_OF_IPV4_SRC	/* IPv4 source address. */	N	N	N	N	
		OXM_OF_IPV4_DST	/* IPv4 destination address. */	N	N	N	N	
		OXM_OF_TCP_SRC	/* TCP source port. */	N	N	N	N	
		OXM_OF_TCP_DST	/* TCP destination port. */	N	N	N	N	
		OXM_OF_UDP_SRC	/* UDP source port. */	N	N	N	N	
		OXM_OF_UDP_DST	/* UDP destination port. */	N	N	N	N	
		OXM_OF_SCTP_SRC	/* SCTP source port. */	N	N	N	N	
		OXM_OF_SCTP_DST	/* SCTP destination port. */	N	N	N	N	
		OXM_OF_ICMPV4_TYPE	/* ICMP type. */	N	N	N	N	
		OXM_OF_ICMPV4_CODE	/* ICMP code. */	N	N	N	N	
		OXM_OF_ARP_OP	/* ARP opcode. */	Y	Y	Y	Y	
		OXM_OF_ARP_SPA	/* ARP source IPv4 address. */	Y	Y	Y	Y	
		OXM_OF_ARP_TPA	/* ARP target IPv4 address. */	Y	Y	Y	Y	
		OXM_OF_ARP_SHA	/* ARP source hardware address. */	Y	Y	Y	Y	
		OXM_OF_ARP_THA	/* ARP target hardware address. */	Y	Y	Y	Y	
		OXM_OF_IPV6_SRC	/* IPv6 source address. */	N	N	N	N	
		OXM_OF_IPV6_DST	/* IPv6 destination address. */	N	N	N	N	
		OXM_OF_IPV6_FLABEL	/* IPv6 Flow Label */	N	N	N	N	
		OXM_OF_ICMPV6_TYPE	/* ICMPv6 type. */	N	N	N	N	
		OXM_OF_ICMPV6_CODE	/* ICMPv6 code. */	N	N	N	N	
		OXM_OF_IPV6_ND_TARGET	/* Target address for ND. */	N	N	N	N	
		OXM_OF_IPV6_ND_SLL	/* Source link-layer for ND. */	N	N	N	N	
		OXM_OF_IPV6_ND_TLL	/* Target link-layer for ND. */	N	N	N	N	
		OXM_OF_MPLS_LABEL	/* MPLS label. */	Y	Y	Y	Y	
		OXM_OF_MPLS_TC	/* MPLS TC. */	Y	Y	Y	Y	
A.3	Controller-to-Switch Messages							
A.3.1	Handshake	Datapath_id	The datapath_id field uniquely identifies a datapath. The lower 48 bits are intended for the switch MAC address, while the top 16 bits are up to the implementer.	Y	Y	Y	Y	
			Use datapath_id to distinguish multiple virtual switch instances on a single physical switch.	Y	Y	Y	Y	
		Capabilities supported by the datapath	OFPC_FLOW_STATS = 1 << 0, /* Flow statistics. */	Y	Y	Y	Y	
			OFPC_TABLE_STATS = 1 << 1, /* Table statistics. */	Y	Y	Y	Y	
			OFPC_PORT_STATS = 1 << 2, /* Port statistics. */	Y	Y	Y	Y	
			OFPC_GROUP_STATS = 1 << 3, /* Group statistics. */	Y	Y	Y	Y	
			OFPC_IP_REASM = 1 << 5, /* Can reassemble IP fragments. */	N	N	N	N	

			OFPC_QUEUE_STATS = 1 << 6, /* Queue statistics. */	N	N	N	N	
			OFPC_PORT_BLOCKED = 1 << 8 /* Switch will block looping ports. */	Y	Y	Y	Y	
A.3.2	Switch Configuration	Controller is able to set and query configuration parameters in the switch with the OFPT_SET_CONFIG and OFPT_GET_CONFIG_REQUEST messages, respectively		Y	Y	Y	Y	
		OFPC_* flags	/* Handling of IP fragments. **/OFPC_FRAG_NORMAL = 0, /** No special handling for fragments. */	Y	Y	Y	Y	
			OFPC_FRAG_DROP = 1 << 0, /* Drop fragments. */	N	N	N	N	
			OFPC_FRAG_REASM = 1 << 1, /* Reassemble (only if OFPC_IP_REASM set). */	N	N	N	N	
			OFPC_FRAG_MASK = 3,	N	N	N	N	
			/* TTL processing - applicable for IP and MPLS packets **/OFPC_INVALID_TTL_TO_CONTROLLER = 1 << 2, /** Send packets with invalid TTL to the controller */	N	N	N	N	
		Miss_send_len	Defines the number of bytes of each packet sent to the controller as a result of flow table miss when configured to generate packet-in messages.	Y	Y	Y	Y	
			If this field equals 0, the switch must send zero bytes of the packet in the ofp_packet_in message.	Y	Y	Y	Y	
			If the value is set to OFPCML_NO_BUFFER the complete packet must be included in the message, and should not be buffered.	Y	Y	Y	Y	
A.3.3	Flow Table Configuration	Flow tables are numbered from 0 and can take any number until OFPTT_MAX	OFPTT_MAX = 0xfe	Y	Y	Y	Y	
		Controller can configure and query table state in the switch with the OFP_TABLE_MOD and OFPST_TABLE_STATS requests, respectively	The switch responds to a table stats request with aOFPT_STATS_REPLY message.	Y	Y	Y	Y	
		OFP_TABLE_MOD	If the table_id is OFPTT_ALL, the configuration is applied to all tables in the switch.	Y	Y	Y	Y	
		Config field is a bitmap that is used to configure the default behavior of unmatched packets	OFPTC_TABLE_MISS_CONTROLLER = 0, /* Send to controller. */	Y	Y	Y	Y	
			OFPTC_TABLE_MISS_CONTINUE = 1 << 0, /* Continue to the next table in the pipeline (OpenFlow 1.0 behavior). */	Y	Y	Y	Y	
			OFPTC_TABLE_MISS_DROP = 1 << 1, /* Drop the packet. */	Y	Y	Y	Y	
			OFPTC_TABLE_MISS_MASK = 3	Y	Y	Y	Y	
A.3.4	Modify State Messages	Modifications to a flow table from the controller are done with the OFPT_FLOW_MOD message		Y	Y	Y	Y	
		Modifications to the group table from the controller are done with the OFPT_GROUP_MOD message		Y	Y	Y	Y	
		The controller uses the OFPT_PORT_MOD message to modify the behavior of the port		Y	Y	Y	Y	
A.3.5	Read State Messages	While the system is running, the datapath may be queried about its current state using the OFPT_STATS_REQUEST message	/* Description of this OpenFlow switch.* The request body is empty.* The reply body is struct ofp_desc_stats. **/OFPST_DESC = 0, /** Body of reply to OFPST_DESC request. Each entry is a NULL- terminated ASCII string. **/struct ofp_desc_stats {char mfr_desc[DESC_STR_LEN]; /** Manufacturer description. **/char hw_desc[DESC_STR_LEN]; /**	Y	Y	Y	Y	

			Hardware description. **/char sw_desc[DESC_STR_LEN]; /** Software description. **/char serial_num[SERIAL_NUM_LEN]; /** Serial number. **/char dp_desc[DESC_STR_LEN]; /** Human readable description of datapath. */};					
			/* Individual flow statistics. The request body is struct ofp_flow_stats_request. The reply body is an array of struct ofp_flow_stats. **/OFPST_FLOW = 1, /** Body of reply to OFPST_FLOW request. **/struct ofp_flow_stats {uint16_t length; /** Length of this entry. **/uint8_t table_id; /** ID of table flow came from. **/uint8_t pad;uint32_t duration_sec; /** Time flow has been alive in seconds. **/uint32_t duration_nsec; /** Time flow has been alive in nanoseconds beyondduration_sec. **/uint16_t priority; /** Priority of the entry. **/uint16_t idle_timeout; /** Number of seconds idle before expiration. **/uint16_t hard_timeout; /** Number of seconds before expiration. **/uint8_t pad2[6]; /** Align to 64-bits. **/uint64_t cookie; /** Opaque controller-issued identifier. **/uint64_t packet_count; /** Number of packets in flow. **/uint64_t byte_count; /** Number of bytes in flow. **/struct ofp_match match; /** Description of fields. Variable size. **///struct ofp_instruction instructions[0]; /** Instruction set. */};	Y	Y	Y	Y	
			/* Aggregate flow statistics. The request body is struct ofp_aggregate_stats_request. The reply body is struct ofp_aggregate_stats_reply. **/OFPST_AGGREGATE = 2, /** Body of reply to OFPST_AGGREGATE request. **/struct ofp_aggregate_stats_reply {uint64_t packet_count; /** Number of packets in flows. **/uint64_t byte_count; /** Number of bytes in flows. **/uint32_t flow_count; /** Number of flows. **/uint8_t pad[4]; /** Align to 64 bits. */};	Y	Y	Y	Y	
			/* Flow table statistics. The request body is empty. The reply body is an array of struct ofp_table_stats. **/OFPST_TABLE = 3, /** Body of reply to OFPST_TABLE request. **/struct ofp_table_stats {uint8_t table_id; /** Identifier of table. Lower numbered tables are consulted first. **/uint8_t pad[7]; /** Align to 64-bits. **/char name[OFP_MAX_TABLE_NAME_LEN];uint64_t match; /** Bitmap of (1 << OFPXMT_**) that indicate the fields the table can match on. */uint64_t wildcards; /** Bitmap of (1 << OFPXMT_**) wildcards that are supported by the table. */uint32_t write_actions; /** Bitmap of OFPAT_* that are supported by the table with OFPIT_WRITE_ACTIONS. **/uint32_t apply_actions; /** Bitmap of OFPAT_* that are supported by the table with OFPIT_APPLY_ACTIONS. **/uint64_t write_setfields;/** Bitmap of (1 << OFPXMT_**) header fields that can be set with OFPIT_WRITE_ACTIONS. */uint64_t apply_setfields;/** Bitmap of (1 << OFPXMT_**) header fields that can be set with OFPIT_APPLY_ACTIONS. */uint64_t metadata_match; /** Bits of metadata table can match. **/uint64_t metadata_write; /** Bits of metadata table can write. **/uint32_t instructions; /** Bitmap of OFPIT_* values supported. **/uint32_t config; /** Bitmap of OFPTC_* values **/uint32_t max_entries; /** Max number of entries supported. **/uint32_t active_count; /** Number of active entries. **/uint64_t lookup_count; /** Number of packets looked up in table. **/uint64_t matched_count; /** Number of packets that hit table. */};	Y	Y	Y	Y	
			/* Port statistics. The request body is struct ofp_port_stats_request. The reply body is an array of struct ofp_port_stats. **/OFPST_PORT = 4, /** Body of reply to OFPST_PORT request. If a counter is unsupported, set the field to all ones. **/struct ofp_port_stats {uint32_t port_no;uint8_t pad[4]; /** Align to 64-bits. **/uint64_t rx_packets; /** Number of received packets. **/uint64_t tx_packets; /** Number of transmitted packets. **/uint64_t rx_bytes; /** Number of received bytes. **/uint64_t tx_bytes; /** Number of transmitted bytes. **/uint64_t rx_dropped; /** Number of packets dropped by RX. **/uint64_t tx_dropped; /** Number of packets dropped by TX. **/uint64_t rx_errors; /** Number of receive errors. This is a super-set of more specific receive errors and should be greater than or	Y	Y	Y	Y	

			equal to the sum of all rx_***err values. */uint64_t tx_errors; /*** *Number of transmit errors. This is a super-set of more specific transmit errors and should be greater than or equal to the sum of all tx*_**err values (none currently defined.) */uint64_t rx_frame_err; /** Number of frame alignment errors. **/uint64_t rx_over_err; /** Number of packets with RX overrun. **/uint64_t rx_crc_err; /** Number of CRC errors. **/uint64_t collisions; /** Number of collisions. */};					
			/* Queue statistics for a port The request body is struct ofp_queue_stats_request. The reply body is an array of struct ofp_queue_stats **/OFPST_QUEUE = 5, The body of the reply consists of an array of the following structure:struct ofp_queue_stats {uint32_t port_no;uint32_t queue_id; /** Queue i.d **/uint64_t tx_bytes; /** Number of transmitted bytes. **/uint64_t tx_packets; /** Number of transmitted packets. **/uint64_t tx_errors; /** Number of packets dropped due to overrun. */};	N	N	N	N	
			/* Group features. The request body is empty. The reply body is struct ofp_group_features_stats. **/OFPST_GROUP_FEATURES = 8, /** Body of reply to OFPST_GROUP_FEATURES request. Group features. **/struct ofp_group_features_stats {uint32_t types; /** Bitmap of OFPGT_* values supported. **/uint32_t capabilities; /** Bitmap of OFPGFC_* capability supported. **/uint32_t max_groups[4]; /** Maximum number of groups for each type. **/uint32_t actions[4]; /** Bitmaps of OFPAT_* that are supported. */};	Y	Y	Y	Y	
			/* Experimenter extension. The request and reply bodies begin with* struct ofp_experimenter_stats_header. The request and reply bodies are otherwise experimenter-defined. **/OFPST_EXPERIMENTER = 0xffff /** Body for ofp_stats_request/reply of type OFPST_EXPERIMENTER. **/struct ofp_experimenter_stats_header {uint32_t experimenter; /** Experimenter ID which takes the same form as in struct ofp_experimenter_header. **/uint32_t exp_type; /** Experimenter defined. **//** Experimenter-defined arbitrary additional data. */};	Y	Y	Y	Y	
A.3.6	Queue Configuration Messages	Queue configuration takes place outside the OpenFlow protocol, either through a command line tool	CLI support	Y	Y	Y	Y	
		The switch replies back with an ofp_queue_get_config_reply command, containing a list of configured queues	/* Queue configuration for a given port. **/struct ofp_queue_get_config_reply {struct ofp_header header;uint32_t port;uint8_t pad[4];struct ofp_packet_queue queues[0]; /** List of configured queues. */};	N	N	Y	N	
A.3.7	Packet-Out Message	When the controller wishes to send a packet out through the datapath, it uses the OFPT_PACKET_OUT message		Y	Y	Y	Y	
A.3.8	Barrier Message	When the controller wants to ensure message dependencies have been met or wants to receive notifications for completed operations, it may use an OFPT_BARRIER_REQUEST message	Upon receipt, the switch must finish processing all previously-received messages, including sending corresponding reply or error messages, before executing any messages beyond the Barrier RequestRequest. When such processing is complete, the switch must send an OFPT_BARRIER_REPLY message with the xid of the original request.	Y	Y	Y	Y	
A.3.9	Role Request Message	When the controller wants to change its role, it uses the OFPT_ROLE_REQUEST message and can have the following values	OFPCR_ROLE_NOCHANGE = 0, /* Don't change current role. */	Y	Y	Y	Y	
			OFPCR_ROLE_EQUAL = 1, /* Default role, full access. */	Y	Y	Y	Y	
			OFPCR_ROLE_MASTER = 2, /* Full access, at most one master. */	Y	Y	Y	Y	
			OFPCR_ROLE_SLAVE = 3, /* Read-only access. *	Y	Y	Y	Y	

A.4	Asynchronous Messages							
A.4.1	Packet-In Message	Switches that implement buffering are expected to expose, through documentation, both the amount of available buffering, and the length of time before buffers may be reused	A switch should prevent a buffer from being reused until it has been handled by the controller, or some amount of time (indicated in documentation) has passed.	Y	Y	Y	Y	
A.4.2	Flow Removed Message	If the controller has requested to be notified when flows time out or are deleted from tables, the datapath does this with the OFPT_FLOW_REMOVED message	The reason field is one of the following:OFPRR_IDLE_TIMEOUT = 0, /* Flow idle time exceeded idle_timeout. **/OFPRR_HARD_TIMEOUT = 1, /** Time exceeded hard_timeout. **/OFPRR_DELETE = 2, /** Evicted by a DELETE flow mod. **/OFPRR_GROUP_DELETE = 3, /** Group was removed. */	Y	Y	Y	Y	
A.4.3	Port Status Message	As ports are added, modified, and removed from the datapath, the controller needs to be informed with the OFPT_PORT_STATUS message	The status can be one of the following values:OFPPR_ADD = 0, /* The port was added. **/OFPPR_DELETE = 1, /** The port was removed. **/OFPPR_MODIFY = 2, /** Some attribute of the port has changed. */	Y	Y	Y	Y	
A.4.4	Error Message	There are times that the switch needs to notify the controller of a problem. This is done with the OFPT_ERROR_MSG message	Currently defined error types are:OFPET_HELLO_FAILED = 0, /* Hello protocol failed. **/OFPET_BAD_REQUEST = 1, /** Request was not understood. **/OFPET_BAD_ACTION = 2, /** Error in action description. **/OFPET_BAD_INSTRUCTION = 3, /** Error in instruction list. **/OFPET_BAD_MATCH = 4, /** Error in match. **/OFPET_FLOW_MOD_FAILED = 5, /** Problem modifying flow entry. **/OFPET_GROUP_MOD_FAILED = 6, /** Problem modifying group entry. **/OFPET_PORT_MOD_FAILED = 7, /** Port mod request failed. **/OFPET_TABLE_MOD_FAILED = 8, /** Table mod request failed. **/OFPET_QUEUE_OP_FAILED = 9, /** Queue operation failed. **/OFPET_SWITCH_CONFIG_FAILED = 10, /** Switch config request failed. **/OFPET_ROLE_REQUEST_FAILED = 11, /** Controller Role request failed. **/OFPET_EXPERIMENTER = 0xffff /** Experimenter error messages. */	Y	Y	Y	Y	
A.5	Symmetric Messages	See Section 6.1.3		Y	Y	Y	Y	
B	Appendix B Release Notes							
B.6.6	Vendor Extensions	Vendors are now able to add their own extensions, while still being OpenFlow compliant. The primary way to do this is with the new OFPT_VENDOR message type		N	N	N	N	
B.6.8	802.1D Spanning Tree	A switch that implements STP must set the new OFPC_STP bit in the 'capabilities' field of its OFPT_FEATURES_REPLY message.	A switch that implements STP at all must make it available on all of its physical ports, but it need not implement it on virtual ports (e.g. OFPP_LOCAL)	Y	Y	Y	Y	
			The complete set of port configuration flags are:OFPPC_PORT_DOWN = 1 << 0, /* Port is administratively down. **/OFPPC_NO_STP = 1 << 1, /** Disable 802.1D spanning tree on port. **/OFPPC_NO_RECV = 1 << 2, /** Drop most packets received on port. **/OFPPC_NO_RECV_STP = 1 << 3, /** Drop received 802.1D STP packets. **/OFPPC_NO_FLOOD = 1 << 4, /** Do not include this port when flooding. **/OFPPC_NO_FWD = 1 << 5, /** Drop packets forwarded to port. **/OFPPC_NO_PACKET_IN = 1 << 6 /** Do not send packet-in msgs for port. */	Y	Y	Y	Y	
		Packets received on ports that are disabled by spanning tree must follow the normal flow table processing path		Y	Y	Y	Y	

B.6.21	Behavior Defined When Controller Connection Lost	In the case that the switch loses contact with the controller, the default behavior must be to do nothing - to let flows timeout naturally. Other behaviors can be implemented via vendor-specific command line interface or vendor extension OpenFlow messages	Default behavior supported.	Y	Y	Y	Y	
B.7.1	Failover	Switch can be configured with a list of controllers. If the first controller fails, it will automatically switch over to the second controller on the list		Y	Y	Y	Y	
B.7.2	Emergency Flow Cache	The protocol and reference implementation have been extended to allow insertion and management of emergency flow entries. Emergency-specific flow entries are inactive until a switch loses connectivity from the controller	The switch invalidates all normal flow table entries and copies all emergency flows into the normal flow table. Upon connecting to a controller again, all entries in the flow cache stay active. The controller then has the option of resetting the flow cache if needed.	N	N	N	N	
B.7.9	Rewrite DSCP in IP ToS header	Added Flow action to rewrite the DiffServ CodePoint bits part of the IP ToS field in the IP header.	This enables basic support for basic QoS with OpenFlow in in some switches.	Y	Y	Y	Y	
B.8.1	Slicing	OpenFlow now supports multiple queues per output port. Queues support the ability to provide minimum bandwidth guarantees	The bandwidth allocated to each queue is configurable.	Y	Y	Y	Y	
B.9	OpenFlow version 1.1							
B.9.1	Multiple Tables	The switch now expose a pipeline with multiple tables.		Y	Y	Y	Y	
		Flow entry have instruction to control pipeline processing		Y	Y	Y	Y	
		Controller can choose packet traversal of tables via goto instruction		Y	Y	Y	Y	
		Metadata field (64 bits) can be set and match in tables		N	N	N	N	
		Packet actions can be merged in packet action set		N	N	N	N	
		Packet action set is executed at the end of pipeline		Y	Y	Y	Y	
		Packet actions can be applied between table stages		N	N	N	N	
		Table miss can send to controller, continue to next table or drop	To controller only.	N	N	N	N	
		Rudimentary table capability and configuration		N	N	N	N	
B.9.2	Groups	Group indirection to represent a set of ports		Y	Y	Y	Y	
		Group table with 4 types of groups :	All - used for multicast and flooding.	Y	Y	Y	Y	
			Select - used for multipath.	N	N	Y	Y	
			Indirect - simple indirection.	Y	Y	Y	Y	
			Fast Failover - use first live port.	N	N	Y	Y	
		Group action to direct a flow to a group		Y	Y	Y	Y	
B.9.3	Tags: MPLS & VLAN	Support for VLAN and QinQ, adding, modifying and removing VLAN headers		N	N	Y	N	
		Support for MPLS, adding, modifying and removing MPLS shim headers		Y	Y	Y	Y	

B.9.4	Virtual ports	Make port number 32 bits, enable larger number of ports	GRE & LAG	Y	Y	Y	Y	LOCAL, GRE,ALL,FLOOD only
		Enable switch to provide virtual port as OpenFlow ports		Y	Y	Y	Y	
		Augment packet-in to report both virtual and physical ports		N	N	Y	N	
B.9.5	Other changes	Remove 802.1d-specific text from spec		N	N	N	N	
		Remove Emergency Flow Cache from spec		N	N	N	N	
		Cookie Enhancements Proposal		N	N	N	N	
		Set queue action (unbundled from output port)		N	N	N	N	
		Maskable DL and NW address match fields		Y	Y	Y	Y	
		Add TTL decrement, set and copy actions for IPv4 and MPLS		N	N	N	N	
		SCTP header matching and rewriting support		N	N	N	N	
		Set ECN action		N	N	N	N	
		Connection interruption trigger fail secure or fail standalone mode		Y	Y	Y	Y	
		Define message handling : no loss, may reorder if no barrier		N	N	N	N	
		Rename VENDOR APIs to EXPERIMENTER APIs						
B.10	OpenFlow version 1.2							
B.10.1	Extensible match support	The Extensible set_field action reuses the OXM encoding defined for matches, and enables to rewrite any header field in a single action (EXT-13)	Deprecate most header rewrite actions.	N	N	N	N	
			Introduce generic set-field action (EXT-13).	N	N	N	N	
			Reuse match TLV structure (OXM) in set-field action.	N	N	N	N	
B.10.2	Extensible 'set field' packet rewriting support	Rather than introduce a hard coded field in the packet-in message, the flexible OXM encoding is used to carry packet context	Reuse match TLV structure (OXM) to describe metadata in packet-in (EXT-6).	N	N	N	N	Layer-2 field supported
			Include the 'metadata' field in packet-in.	N	N	N	N	
			Move ingress port and physical port from static field to OXM encoding.	N	N	N	N	
			Allow to optionally include packet header fields in TLV structure.	N	N	N	N	
B.10.3	Extensible context expression in 'packet-in'	Rather than introduce a hard coded field in the packet-in message, the flexible OXM encoding is used to carry packet context	Reuse match TLV structure (OXM) to describe metadata in packet-in (EXT-6).	Y	Y	Y	Y	
			Include the 'metadata' field in packet-in.	Y	Y	Y	Y	
			Move ingress port and physical port from static field to OXM encoding.	Y	Y	Y	Y	
			Allow to optionally include packet header fields in TLV structure.	Y	Y	Y	Y	
B.10.4	Extensible Error messages via	An experimenter error code has been added, enabling experimenter functionality to generate custom error messages (EXT-		N	N	N	N	

	experimenter error type	2). The format is identical to other experimenter APIs						
B.10.5	IPv6 support added	Basic support for IPv6 match and header rewrite has been added	Added support for matching on IPv6 source address, destination address, protocol number, traffic class, ICMPv6 type, ICMPv6 code and IPv6 neighbor discovery header fields (EXT-1).	Y	Y	Y	Y	IPv6_SIP + IPv6_DIP; IPv6_SIP + MAC DA + MAC SA; IPv6_DIP + MAC DA + MAC SA; 512 flow for P-3780 & P-3920
			Added support for matching on IPv6 flow label (EXT-36).	N	N	N	N	
B.10.6	Simplified behaviour of flow-mod request	The behaviour of flow-mod request has been simplified (EXT-30)	MODIFY and MODIFY STRICT commands never insert new flows in the table.	N	N	N	N	
			New flag OFPFF RESET COUNTS to control counter reset.	N	N	N	N	
			Remove quirky behaviour for cookie field.	Y	Y	Y	Y	
B.10.7	Removed packet parsing specification	The match fields are only defined logically	OpenFlow does not mandate how to parse packets.	N	N	N	N	
			Parsing consistency achieved via OXM pre-requisite.	N	N	N	N	
B.10.8	Controller role change mechanism	The controller role change mechanism is a simple mechanism to support multiple controllers for failover (EXT-39)	The switch only need to remember the role of each controller to help the controller election mechanism.	N	N	N	N	
			Simple mechanism to support multiple controllers for failover.	Y	Y	Y	Y	
			Switches may now connect to multiple controllers in parallel.	Y	Y	Y	Y	
			Enable each controller to change its roles to equal, master or slave.	Y	Y	Y	Y	
B.10.9	Other changes	Per-table metadata bitmask capabilities (EXT-34)		Y	Y	Y	Y	
		Rudimentary group capabilities (EXT-61)		N	N	N	N	
		Add hard timeout info in flow-removed messages (OFP-283)		Y	Y	Y	Y	
		Add ability for controller to detect STP support(OFP-285)		Y	Y	Y	Y	
		Turn off packet buffering with OFPCML NO BUFFER (EXT-45)		Y	Y	Y	Y	
		Added ability to query all queues (EXT-15)		N	N	N	N	
		Added experimenter queue property (EXT-16)		Y	Y	Y	Y	
		Added max-rate queue property (EXT-21)		Y	Y	Y	Y	
		Enable deleting flow in all tables (EXT-10)		Y	Y	Y	Y	
		Enable switch to check chaining when deleting groups (EXT-12)		N	N	N	N	
		Enable controller to disable buffering (EXT-45)		Y	Y	Y	Y	
		Virtual ports renamed logical ports (EXT-78)		N	N	N	N	
		New error messages (EXT-1, EXT-2, EXT-12, EXT-13, EXT-39, EXT-74 and EXT-82)		Y	Y	Y	Y	
		Include release notes into the specification document		Y	Y	Y	Y	
		Many other bug fixes, rewording and clarifications		Y	Y	Y	Y	

	OpenFlow 1.3							
	Per flow meters	Flexible meter framework based on per-flow meters and meter bands.						
		Meter statistics, including per band statistics.	1 band per meter	Y	Y	Y	Y	
		Enable to attach meters flexibly to flow entries.		Y	Y	Y	Y	
		◖Simple rate-limiter support (drop packets		Y	Y	Y	Y	
	Per connection event filtering	Add asynchronous message filter for each controller connection		Y	Y	Y	Y	
	Per connection event filtering	Add asynchronous message filter for each controller connection						
		Set default lter value to match OpenFlow 1.2 behaviour		Y	Y	Y	Y	
		Remove OFPC_INVALID_TTL_TO_CONTROLLER config flag						
	Auxiliary connections	Auxiliary connections are mostly useful to carry packet-in and packet-out messages		N	N	N	N	
	MPLS BoS matching	match the Bottom of Stack bit (BoS) from the MPLS header (EXT-85). The BoS bit indicates if other MPLS shim header are in the payload of the present MPLS packet, and matching this bit can help to disambiguate case where the MPLS label is present MPLS packet, and matching this bit can help to disambiguate case where the MPLS label is reused across levels of MPLS encapsulation		N	N	N	N	
	Provider Backbone Bridging tagging	Push and Pop operation to add PBB header as a tag.◖		Y	Y	Y	Y	
		New OXM field to match I-SID for the PBB header	PBB-MPLS-VLAN order	N	N	N	N	
	Rework tag order	the nal order of tags in a packet is dictated by the order of the taggingoperations, each tagging operation adds its tag in the outermost position	Remove defined order of tags in packet from the specification.	N	N	N	N	
			Tags are now always added in the outermost possible position.	Y	Y	Y	Y	
			Action-list can add tags in arbitrary order.	N	N	N	N	
			◖Tag order is predened for tagging in the action-set.	Y	Y	Y	Y	
	Tunnel-ID metadata	A new OXM field that expose to the OpenFlow pipeline metadata associated with the logical port, most commonly the demultiplexing eld from the encapsulation header	If the logical port perform GRE encapsulation, the tunnel-id eld would map to the GRE key field from the GRE header. be able to match the GRE key in the tunnel-id match eld.	N	N	N	N	
	Cookies in packet-in							
	Duration for stats	Duration field was added to most statistics, including port statistics, group statistics, queue statistics and meter statistics		Y	Y	Y	Y	
	On demand flow counters	New flow-mod flags have been added to disable packet and byte counters on a per-flow basis		N	N	N	N	

PicOS Support for OpenFlow 1.3.0

This document contains OpenFlow 1.3.0 features supported by the Pica8 PicOS software. For clarity, the feature names in this table are identical to the feature names found in OpenFlow Switch Specification Version 1.3.0.

OpenFlow Messages

Each OpenFlow message begins with the OpenFlow header. The OpenFlow header has several fields, including the **type** field. The **type** field identifies the type of OpenFlow message.

The OpenFlow protocol has three message types: *symmetric*, *controller-to-switch*, *asynchronous*. Each message type has multiple sub-types.

Symmetric Messages

Symmetric messages are unsolicited messages that may be initiated by either the switch or the controller. Symmetric messages are sent without explicit solicitation, in either direction. The following table describes PicOS support for symmetric messages:

Table 1 PicOS Support for OpenFlow Symmetric Messages

Message	Support	Comments
OFPT_HELLO	Supported	
OFPT_ERROR	Supported	
OFPT_ECHO_REQUEST	Supported	
OFPT_ECHO_REPLY	Supported	
OFPT_EXPERIMENTER	Not Supported	

Controller-to-Switch Messages

Controller-to-switch messages are sent from the controller to the switch. These messages are used to directly manage the state of a switch. Controller-to-switch messages may or may not require a response from the switch.

The following table describes PicOS support for controller-to-switch messages:

Table 2 PicOS Support for OpenFlow Controller-to-Switch Messages

Message	Support	Comments
OFPT_FEATURES_REQUEST	Supported	
OFPT_FEATURES_REPLY See Capabilities Supported by Datapath		
OFPT_GET_CONFIG_REQUEST	Supported	
OFPT_GET_CONFIG_REPLY		
OFPT_SET_CONFIG	Supported	
OFPT_PACKET_OUT	Supported	
OFPT_FLOW_MOD	Supported	
OFPT_GROUP_MOD	Supported	
OFPT_PORT_MOD	Supported	
OFPT_TABLE_MOD	Supported	
OFPT_MULTIPART_REQUEST See Multipart Messages	Supported	
OFPT_MULTIPART_REPLY See Multipart Messages	Supported	
OFPT_BARRIER_REQUEST	Supported	
OFPT_BARRIER_REPLY		
OFPT_QUEUE_GET_CONFIG_REQUEST	Supported	
OFPT_QUEUE_GET_CONFIG_REPLY	Supported	
OFPT_ROLE_REQUEST	Supported	
OFPT_ROLE_REPLY		

Message	Support	Comments
OFPT_GET_ASYNC_REQUEST	Supported	
OFPT_GET_ASYNC_REPLY	Supported	
OFPT_SET_ASYNC	Supported	
OFPT_METER_MOD	Supported	

Asynchronous Messages

Asynchronous messages are sent from the switch to the controller. These messages are used to communicate network events and switch state changes to the controller. Asynchronous messages are sent without a controller explicitly requesting them from a switch.

The following table describes PicOS support for asynchronous messages:

Table 3 PicOS Support for OpenFlow Asynchronous Messages

Message	Support	Comments
OFPT_PACKET_IN	Supported	
OFPT_FLOW_REMOVED	Supported	
OFPT_PORT_STATUS	Supported	

Multipart Messages

The following table describes PicOS support for multipart messages: a single OpenFlow message cannot be larger than 64 kilobytes. Multipart messages are used to encode requests or replies that would carry a large amount of data, and would not always fit in a single OpenFlow message. The sender encodes the request or reply as a sequence of multipart messages, with a specific multipart type. The receiver re-assembles the request or reply.

Table 4 PicOS Support for OpenFlow Multipart Messages

Message	Support	Comments
OFPMP_DESC	Supported	
OFPMP_FLOW	Supported	
OFPMP_AGGREGATE		
OFPMP_TABLE	Supported	
OFPMP_PORT_STATS	Supported	
OFPMP_QUEUE	Supported	
OFPMP_GROUP	Supported	
OFPMP_GROUP_DESC	Supported	
OFPMP_GROUP_FEATURES	Not Supported	
OFPMP_METER	Supported	
OFPMP_METER_CONFIG	Supported	
OFPMP_METER_FEATURES	Supported	
OFPMP_TABLE_FEATURES	Supported	
OFPMT_PORT_DESC	Supported	
OFPMP_EXPERIMENTER	Not Supported	

Capabilities Supported by Datapath

The controller sends an **OFPT_FEATURES_REQUEST** message to the switch, once a session is established. The switch responds to the **OFPT_FEATURES_REQUEST** message with an **OFPT_FEATURES_REPLY** message. The **OFPT_FEATURES_REPLY** message has several fields, including the **capabilities** field. The **capabilities** field identifies the capabilities supported by the switch datapath.

The **capabilties** field is a combination of the following bits/flags:

Table 5 PicOS Support for OpenFlow Capabilities Supported by Datapath

Specification	Support	Comments
OFPC_FLOW_STATS	Supported	
OFPC_TABLE_STATS	Supported	
OFPC_PORT_STATS	Supported	
OFPC_GROUP_STATS	Supported	

Specification	Support	Comments
OFPC_IP_REASM		
OFPC_QUEUE_STATS		
OFPC_PORT_BLOCKED		

OpenFlow Ports

OpenFlow ports are abstract network interfaces used for passing traffic between the OpenFlow switch and the rest of the network. An OpenFlow switch makes a number of OpenFlow ports available. The set of OpenFlow ports does not have to be identical to the set of physical network interfaces on the switch hardware.

Port Descriptions

The OpenFlow switch receives and sends packets on OpenFlow ports. The switch may define physical and logical ports, and the OpenFlow specification also defines some reserved ports.

Table 6 PicOS Support for OpenFlow Ports

Specification	Support	Comments
OFPP_MAX		
OFPP_IN_PORT	Supported	
OFPP_TABLE	Supported	
OFPP_NORMAL	Supported	
OFPP_FLOOD	Supported	
OFPP_ALL	Supported	
OFPP_CONTROLLER	Supported	
OFPP_LOCAL	Supported	
OFPP_ANY	Supported	

Port Administrative Settings

The following table describes PicOS support for administrative settings of OpenFlow ports:

Table 7 PicOS Support for OpenFlow Port Administrative Settings

Specification	Support	Comments
OFPPC_PORT_DOWN	Supported	
OFPPC_NO_STP	Supported	
OFPPC_NO_RECV	Supported	
OFPPC_NO_RECV_STP	Supported	
OFPPC_NO_FLOOD		
OFPPC_NO_FWD		
OFPPC_NO_PACKET_IN		

Port States

The following table describes PicOS support for OpenFlow port states:

Table 8 PicOS Support for OpenFlow Port States

Specification	Support	Comments
OFPPS_LINK_DOWN	Supported	
OFPPS_BLOCKED		
OFPPS_LIVE		

Port Features

The following table describes PicOS support for OpenFlow port features available in the datapath:

Table 9 PicOS Support for OpenFlow Port Features

Specification	Support	Comments
OFPPF_10MB_HD	Supported	
OFPPF_10MB_FD	Supported	
OFPPF_100MB_HD	Supported	
OFPPF_100MB_FD	Supported	
OFPPF_1GB_HD	Supported	
OFPPF_1GB_FD	Supported	
OFPPF_10GB_FD	Supported	
OFPPF_40GB_FD	Supported	
OFPPF_100GB_FD	Supported	
OFPPF_1TB_FD		
OFPPF_OTHER		
OFPPF_COPPER	Supported	
OFPPF_FIBER	Supported	
OFPPF_AUTONEG	Supported	
OFPPF_PAUSE	Supported	
OFPPF_PAUSE_ASYM		

OpenFlow Instructions

Each flow entry contains a set of instructions that are executed when a packets matches the entry. The following table details OpenFlow instructions supported by PicOS:

Table 10 PicOS Support for OpenFlow Instructions

Specification	Support	Comments
OFPIT_GOTO_TABLE	Supported	
OFPIT_WRITE_METADATA	Supported	
OFPIT_WRITE_ACTIONS	Supported	
OFPIT_APPLY_ACTIONS	Supported	
OFPIT_CLEAR_ACTIONS	Supported	
OFPIT_METER	Supported	
OFPIT_EXPERIMENTER		

OpenFlow Action Types

The following table details OpenFlow action types supported by PicOS:

Table 11 PicOS Support for OpenFlow Action Types

Specification	Support	Comments
OFPAT_OUTPUT	Supported	
OFPAT_COPY_TTL_OUT	Supported	
OFPAT_COPY_TTL_IN	Supported	
OFPAT_SET_MPLS_TTL	Supported	
OFPAT_DEC_MPLS_TTL	Not Supported	
OFPAT_PUSH_VLAN	Supported	
OFPAT_POP_VLAN	Supported	
OFPAT_PUSH_MPLS	Supported	
OFPAT_POP_MPLS	Supported	
OFPAT_SET_QUEUE	Supported	
OFPAT_GROUP	Supported	

Specification	Support	Comments
OFPAT_SET_NW_TTL	Not Supported	
OFPAT_DEC_NW_TTL	Not Supported	
OFPAT_SET_FIELD	Supported	
OFPAT_PUSH_PBB	Supported	
OFPAT_POP_PBB	Supported	
OFPAT_EXPERIMENTER	Not Supported	

OpenFlow Match Fields

A match field may include the packet header, the ingress port, and the metadata value. A match field may use wildcards to match any value, and in some cases bitmasks. A packet is matched against a match field.

The following table details the OXM flow match field types supported by PicOS:

Table 12 PicOS Support for OpenFlow Flow Match Fields

Specification	Support	Comments
OFPXMT_OFB_IN_PORT	Supported	
OFPXMT_OFB_IN_PHY_PORT	Supported	
OFPXMT_OFB_METADATA		
OFPXMT_OFB_ETH_DST	Supported	
OFPXMT_OFB_ETH_SRC	Supported	
OFPXMT_OFB_ETH_TYPE	Supported	
OFPXMT_OFB_VLAN_VID	Supported	
OFPXMT_OFB_VLAN_PCP	Supported	
OFPXMT_OFB_IP_DSCP	Supported	
OFPXMT_OFB_IP_ECN		
OFPXMT_OFB_IP_PROTO	Supported	
OFPXMT_OFB_IPV4_SRC	Supported	
OFPXMT_OFB_IPV4_DST	Supported	
OFPXMT_OFB_TCP_SRC	Supported	
OFPXMT_OFB_TCP_DST	Supported	
OFPXMT_OFB_UDP_SRC	Supported	
OFPXMT_OFB_UDP_DST	Supported	
OFPXMT_OFB_SCTP_SRC		
OFPXMT_OFB_SCTP_DST		
OFPXMT_OFB_ICMPV4_TYPE	Supported	
OFPXMT_OFB_ICMPV4_CODE	Supported	
OFPXMT_OFB_ARP_OP	Supported	
OFPXMT_OFB_ARP_SPA	Supported	
OFPXMT_OFB_ARP_TPA	Supported	
OFPXMT_OFB_ARP_SHA		
OFPXMT_OFB_ARP_THA		
OFPXMT_OFB_IPV6_SRC	Supported	
OFPXMT_OFB_IPV6_DST	Supported	
OFPXMT_OFB_IPV6_FLABEL		
OFPXMT_OFB_ICMPV6_TYPE		
OFPXMT_OFB_ICMPV6_CODE		
OFPXMT_OFB_IPV6_ND_TARGET		

Specification	Support	Comments
OFPXMT_OFB_IPV6_ND_SLL		
OFPXMT_OFB_IPV6_ND_TLL		
OFPXMT_OFB_MPLS_LABEL	Supported	
OFPXMT_OFB_MPLS_TC	Supported	
OFPXMT_OFP_MPLS_BOS		
OFPXMT_OFB_PBB_ISID	Supported	
OFPXMT_OFB_TUNNEL_ID	Supported	
OFPXMT_OFB_IPV6_EXTHDR		

OpenFlow Group Types

The following table describes PicOS support for OpenFlow group types:

Table 13 PicOS Support for OpenFlow Group Types

Specification	Support	Comments
OFPGT_ALL	Supported	
OFPGT_SELECT	Supported	
OFPGT_INDIRECT	Supported	
OFPGT_FF	Supported	

PicOS Support for OpenFlow 1.4

The following table contains OpenFlow 1.4 features supported by PicOS. For clarity, the feature names in this table are identical to the feature names found in OpenFlow Switch Specification Version 1.4.0.

Table 1 OpenFlow 1.4 Features Supported by PicOS

Pica8 OpenFlow V1.4 Compliance Matrix						
Chapter	**Title**	**Features**	**Detail Feature Specification**	**Optional**	**R2.3 Support**	**Remarks**
2	Switch Components	NA				
		Flow table			Y	
		Group table	All, indirect, select, fast_failover group table are all supported.		Y	
		Add/update/delete flow entries			Y	
		Match fields			Y	
		Counters			Y	
		Set of instructions			Y	
4	OpenFlow Ports	NA				
4.1	OpenFlow Ports	see 4.2-4.5			Y	
4.2	Standard Ports	See 4.2-4.5			Y	
4.3	Physical Ports	NA				
		Ingress	PicOS only supports it as matching port.		Y	
		Output			Y	
		Hardware interface			Y	
		Groups			Y	
		Port counters			Y	
4.4	Logical Ports	NA	The OpenFlow logical ports are switch defined ports that don't correspond directly to a hardware interface of the switch.			
		Map to various physical ports			Y	
		LAG			Y	
		Tunnel (GRE)			Y	
		Lookback interface			Y	
		Ingress			Y	
		Output			Y	
		Groups			Y	
4.5	Reserved Ports	NA				
		All	Represents all ports the switch can use for forwarding a specific packet. Can be used only as an output port.		Y	
		Controller	Represents the control channel with the OpenFlow controller. Can be used as an ingress port or as an output port.		Y	
		Table	Represents the start of the OpenFlow pipeline.		Y	
		In_port	Represents the packet ingress port. Can be used only as an output port, send the packet out through its ingress port.		Y	Matching must specify the ingress port.
		Any	Special value used in some OpenFlow commands when no port is specified. Can neither be used as an ingress port nor as an output port.		N	

		Local	Represents the switch's local networking stack and its management stack.	O	Y	
		Normal	Represents the traditional non-OpenFlow pipeline of the switch. Can be used only as an output port and processes the packet using the normal pipeline.	O	Y	
		Flood	Represents flooding using the normal pipeline of the switch. Can be used only as an output port.	O	Y	
5	OpenFlow Tables	NA				
5.1	Pipeline Processing					
		Openflow-only	All packets are processed by the OpenFlow pipeline.		Y	
		Openflow-hybrid	OpenFlow operation and normal Ethernet switching operation.		N	
			L2 Ethernet switching, L3 routing (IPv4 routing, IPv6 routing...), ACL and QoS processing.		N	
			VLAN isolation		N	
			A classification mechanism outside of OpenFlow that routes traffic to either the OpenFlow pipeline or the normal pipeline.		N	
			VLAN tag or input port whether to process the packet using which pipeline.		N	
			Normal and flood		N	
		Multiple flow tables, each flow table containing multiple flow entries			Y	
		Sequentially numbered, start at 0			Y	
		Goto instruction			Y	
		Go forward and not backward			Y	
		Last table can not include goto instruction			N	
		Table miss			Y	
5.2	Flow Table	NA				
		Match fields	To match against packets..		Y	
		Priority	Matching precedence of the flow entry.		Y	
		Counters	Updated when packets are matched.		Y	Only count by Byte
		Instructions	To modify the action set or pipeline processing.		Y	
		Timeouts	Maximum amount of time or idle time before flow is expired by the switch.		Y	
		Cookie	Opaque data value chosen by the controller.		Y	
		Wildcards all fields and priority equal 0 is table-miss			Y	
5.3	Matching	NA				
		Ingress port			Y	
		Metadata fields			N	
		Apply-actions			Y	
		Any			N	
		Highest priority matches packets be selected			Y	
		Counters update and instructions applied			Y	
		OFPFF_CHECK_OVERLAP			Y	
		OFPC_FRAG_REASM			N	
		Behavior when a switch receives a corrupted packet			N	

5.4	Table-miss	NA				
		Every flow table support table-miss			Y	
		Send packets to controller			Y	
		Drop packets			Y	
		Direct packets to a subsequent table			Y	
		Wildcard all match fields			N	MAC/IP/Port can support wildcard.
		Priority= 0			Y	
		Not exist by default			Y	
		Add or remove by controller at any time			Y	
		May expire			N	
		Match packets unmatched by others			Y	
		Instructions applied			Y	
		Packet-in reason is table-miss			Y	
		Packets unmatched are dropped is not exist table-miss			Y	
5.5	Flow Removal	NA				
			Is run by the switch independently of the controller and is based on the state and configuration of flow entries.		Y	
			A non-zero hard_timeout field causes the flow entry to be removed after the given number of seconds, regardless of how many packets it has matched.		Y	
			A non-zero idle_timeout field causes the flow entry to be removed when it has matched no packets in the given number of seconds.		Y	
			The switch must implement flow expiry and remove flow entries from the flow table when one of their timeouts is exceeded.		Y	
		OFPFF_SEND_FLOW_REM flag	When a flow entry is removed, the switch must check the flow entry's OFPFF_SEND_FLOW_REM flag. If this flag is set, the switch must send a flow removed message to the controller.		Y	
			Each flow removed message contains a complete description of the flow entry, the reason for removal (expiry or delete), the flow entry duration at the time of removal, and the flow statistics at time of removal.		Y	
		Eviction	Flow entries may be evicted from flow tables when the switch needs to reclaim resources.		Y	
5.6	Group Table	NA				
		Group identifier			Y	
		Group type			Y	
		Counters			Y	
		Action buckets			Y	
5.6.1	Group Types	All	Used for multicast or broadcast.		Y	
			Effectively cloned for each bucket..		Y	
			Process for each bucket.		Y	Some limitation, please see configuration guide.
			Direct out the ingress, packet is dropped.		Y	
			Output action to OFPP_IN_PORT		Y	Need to specify the in_port in matching.
		Select	Processed by a single bucket.		Y	

			Switch-computed selection algorithm.		Y	
			Bucket weight		N	
			Forward to live ports		Y	
		Indirect	Supports only a single bucket.		Y	
			Multiple flow entries or groups to point to a common group identifier.		Y	
			Supporting faster, more efficient convergence.		N	
			Effectively identical to an all group with one bucket.		Y	
		Fast failover	Execute the first live bucket.		Y	
			Associated with a port and/or group.		Y	
			Change forwarding without request to controller.		Y	
			No bucket live, packet dropped.		Y	
5.7	Meter Table					
		Meter entries			Y	
		Per-flow meters			Y	
		Rate-limit			Y	
		Combine with per-port queue			Y	
		Measure and control packet rate			Y	
		Attached to flow entries			Y	
		In flow instruction set			Y	
		Multiple meters in the same table			Y	
		Multiple meters on the same set of packets			Y	
		Meter identifier			Y	
5.7.1		Meter Bands				
		One band			Y	
		More meter bands			N	
		The rate band applies and the way packets be process			Y	
		Processed by a single meter band based on the current measured meter rate			Y	
		Configure rate lower than current rate			Y	
		No meter band applied if current rate lower than specified rate			Y	
		Band type			Y	
		Rate			Y	
		Counters			Y	
5.8	Counters	NA				
	Per Table Counters	Reference count (active entries)	32 bits		Y	
		Packet Lookups	64 bits		Y	
		Packet Matches	64 bits		Y	
	Per Flow Counters	Received Packets	64 bits		Y	
		Received Bytes	64 bits		Y	
		Duration (seconds)	32 bits		Y	
		Duration (nanoseconds)	32 bits			
	Per Port Counters	Received Packets	64 bits		Y	

		Transmitted Packets	64 bits		Y	
		Received Bytes	64 bits		Y	
		Transmitted Bytes	64 bits		Y	
		Receive Drops	64 bits		Y	
		Transmit Drops	64 bits		Y	
		Receive Errors	64 bits		Y	
		Transmit Errors	64 bits		Y	
		Receive Frame Alignment Errors	64 bits		Y	
		Receive Overrun Errors	64 bits		Y	
		Receive CRC Errors	64 bits		Y	
		Collisions	64 bits		Y	
	Per Queue Counters	Transmit Packets	64 bits		N	
		Transmit Bytes	64 bits		N	
		Transmit Overrun Errors	64 bits		N	
	Per Group Counters	Reference Count (flow entries)	32 bits		Y	
		Packet Count	64 bits		Y	
		Byte Count	64 bits		N	
	Per Bucket Counters	Packet Count	64 bits		N	
		Byte Count	64 bits		N	
5.9	Instructions					
		The controller can query the switch about which of the “Optional Instructions” it supports.			Y	
		Apply-Actions action(s)			Y	
		Clear-Actions			Y	
		Write-Actions action(s)			Y	
		Write-Metadata metadata/mask			Y	
		Goto-Table next-table-id			Y	
		Clear-Actions instruction is executed before the Write-Actions instruction.			Y	
		Goto-Table is executed last.			Y	
		Reject a flow entry if it is unable to execute the instructions & return an unsupported flow error.			N	
5.10	Action Set					
		Action set is associated with each packet.			Y	
		This set is empty by default.			Y	
		Action set is carried between flow tables.			Y	
		When the instruction set of a flow entry does not contain a Goto-Table instruction, pipeline processing stops and the actions in the action set of the packet are executed.			Y	
		Action set contains a maximum of one action of each type.			Y	
		The actions in an action set are applied in the order specified below.			Y	
		1. copy TTL inwards			N	

		2. pop			Y	
		3. push			Y	
		4. copy TTL outwards			N	
		5. decrement TTL			N	
		6. set			Y	
		7. qos			Y	
		8. group	If a group action is specified, apply the actions of the relevant group bucket(s) in the order specified by this list.		Y	
		9. output	If no group action is specified, forward the packet on the port specified by the output action. The output action in the action set is executed last.		N	
			If both an output action and a group action are specified in an action set, the output action is ignored and the group action takes precedence.		N	
			If no output action and no group action were specified in an action set, the packet is dropped.		N	
			The execution of groups is recursive if the switch supports it; a group bucket may specify another group, in which case the execution of actions traverses all the groups specified by the group configuration.		N	
5.11	Action list					
		Apply-Actions instruction and the Packet-out message include an action list	The actions of an action list are executed in the order specified by the list, and are applied immediately to the packet.		Y	
			The effect of those actions is cumulative.		Y	
			If the action list contains an output action, a copy of the packet is forwarded in its current state to the desired port.		Y	
			If the list contains a group actions, a copy of the packet in its current state is processed by the relevant group buckets.		Y	
5.12	Actions					
		Output	Support forwarding to physical ports, switch-defined logical ports and the required reserved ports.		Y	
		Set-Queue	The set-queue action sets the queue id for a packet and is used to provide basic Quality-of-Service (QoS) support.		Y	
		Drop			Y	
		Group			Y	
		Push-Tag/Pop-Tag	Order of header fields - Ethernet, VLAN, MPLS, ARP/IP, TCP/UDP/SCTP (IP-only).		Y	
		Push VLAN header	Push a new VLAN header onto the packet. The Ethertype is used as the Ethertype for the tag. Only Ethertype 0x8100 and 0x88a8 should be used.		Y	
		Pop VLAN header	Pop the outer-most VLAN header from the packet.		Y	
		Push MPLS header	Push a new MPLS shim header onto the packet. Only Ethertype 0x8847 and 0x8848 should be used.		Y	
		Pop MPLS header	Pop the outer-most MPLS tag or shim header from the packet.		Y	
		Push PBB header			Y	
		Pop PBB header			Y	
		Set-Field			Y	
		Set VLAN ID			Y	
		Strip VLAN ID			Y	
		Change-TTL	Modify the values of the IPv4 TTL, IPv6 Hop Limit or MPLS TTL in the packet.		N	

			If it is supported, applied to the outermost-possible header.		N	
		Set MPLS TTL	8 bits: New MPLS TTL, Replace the existing MPLS TTL. Only applies to packets with an existing MPLS shim header.		Y	
		Decrement MPLS TTL	Decrement the MPLS TTL. Only applies to packets with an existing MPLS shim header.		N	
		Set IP TTL	Replace the existing IPv4 TTL or IPv6 Hop Limit and update the IP checksum. Only applies to IPv4 and IPv6 packets.		N	
		Decrement IP TTL	Decrement the IPv4 TTL or IPv6 Hop Limit field and update the IP checksum. Only applies to IPv4 and IPv6 packets		N	
		Copy TTL outwards	Copy the TTL from next-to-outermost to outermost header with TTL. Copy can be IP-to-IP, MPLS-to-MPLS, or IP-to-MPLS.		N	
		Copy TTL inwards	Copy the TTL from outermost to next-to-outermost header with TTL. Copy can be IP-to-IP, MPLS-to-MPLS, or MPLS-to-IP.		N	
5.12.1	Default values for field on push					
		Field values for all fields specified in Table 6 should be copied from existing outer headers to new outer headers.	VLAN ID ← VLAN ID		Y	
		New fields listed in Table 6 without corresponding existing fields should be set to zero.	VLAN priority ← VLAN priority		Y	
		Fields in new headers may be overridden by specifying a “set” action for the appropriate field(s) after the push operation.	MPLS label ← MPLS label		Y	
		Fields in new headers may be overridden by specifying a “set” action for the appropriate field(s) after the push operation.	PBB label ← PBB label		Y	
6	OpenFlow Channel					
6.1	OpenFlow Protocol Overview	The OpenFlow protocol supports three message types, controller-to-switch, asynchronous, and sym-metric, each with multiple sub-types.				
6.1.1		Controller-to-Switch	Controller/switch messages are initiated by the controller and may or may not require a response from the switch.		Y	
6.1.2		Asynchronous	Asynchronous messages are sent without a controller soliciting them from a switch.		Y	
			Switches send asynchronous messages to controllers to denote a packet arrival or switch state change.		Y	
6.1.3		Symmetric	Symmetric messages are sent without solicitation, in either direction., including Hello, Echo, Error, Experimenter message.		Y	
6.2	Message Handling	The OpenFlow protocol provides reliable message delivery and processing, but does not automatically provide acknowledgements or ensure ordered message processing.			Y	
6.3	OpenFlow Channel Connections	The OpenFlow channel is used to exchange OpenFlow message between an OpenFlow switch and an OpenFlow controller.				
6.3.1		Connection Setup	The switch must be able to establish communication with a controller at a user-configurable IP address, using either a user-specified transport port or the default transport port.		Y	

6.3.2		Connection Interruption	In the case that a switch loses contact with all controllers the switch must immediately enter either \fail secure mode" or \fail standalone mode", depending upon the switch implementation and configuration.		Y	
6.3.3		Encryption	The switch and controller may communicate through a TLS connection.		Y	
6.3.4		Multiple Controllers	The switch may establish communication with a single controller, or may establish communication with multiple controllers.		Y	
6.3.5		Auxiliary Connections	The OpenFlow channel may also be composed of a main connection and multiple auxiliary connections.		Y	
6.4	Flow Table Modification Messages	Flow table modification messages are used to add, modify, delete flow.			Y	
6.5	Flow Table Synchronization	A flow table may be synchronized with another flow table. with Flow Table Synchronization			N	
6.6	Group Table Modification Messages	Action of group (including add, modify, delete) can be done by Group table modification messages.			Y	
6.7	Meter Modification Messages	Action of meter (including add, modify, delete) can be done by Meter modification messages.			Y	
6.8	Bundle Messages					
6.8.1		Bundle overview	A bundle is a sequence of OpenFlow modification requests from the controller that is applied as a single OpenFlow operation.		Y	
6.8.2		Bundle example usage			Y	
6.8.3		Bundle error processing	The OpenFlow messages part of a bundle must be pre-validated before they are stored in the bundle.		Y	
6.8.4		Bundle atomic modifications	Committing the bundle must be controller atomic.		N	
6.8.5		Bundle parallelism	The switch must support exchanging echo request and echo reply messages during the creation and population of the bundle, the switch must reply to an echo request without waiting for the end of the bundle.		Y	
7	The OpenFlow Protocol					
7.1	OpenFlow Header	Each Openflow message begins with the OpenFlow header			Y	
7.1.1		Padding	Most OpenFlow messages contain padding fields.		Y	
7.2	Common Structures					
7.2.1		Port Structures	The switch may define physical and logical ports.		Y	
7.2.1.1		Port Description Structures, the physical ports, switch-defined logical ports, and the OFPP_LOCAL reserved port	Ports includes: OFPP_IN_PORT,OFPP_TABLE, OFPP_NORMAL, OFPP_FLOOD, OFPP_ALL, OFPP_CONTROLLER, OFPP_LOCAL,OFPP_ANY		Y	
7.2.1.2		Port Description Properties. A property definition contains the property type, length, and any associated data.	Associated date includes curr, advertised, supported, peer, each one consists of speed, duplexity.		Y	
7.2.2		Flow Match Structures	An OpenFlow match is composed of a flow match header and a sequence of zero or more flow match fields.		Y	
7.2.2.1		Flow Match Header, Fields to match against flows	The flow match header is described by the ofp_match structure, The type field is set to OFPMT_OXM and length field is set to the actual length of ofp_match structure including all match fields. The payload of the OpenFlow match is a set of OXM Flow match fields.		Y	
7.2.2.2		Flow Match Field Structures	The flow match fields are described using the OpenFlow Extensible Match (OXM) format, which is a compact type-length-value (TLV) format.		Y	
7.2.2.3		OXM classes	The match types are structured using OXM match classes, The OpenFlow specification distinguishes two types of OXM match classes, ONF member classes		Y	

			and ONF reserved classes, diferentiated by their high order bit.			
7.2.2.4		Flow Matching	A zero-length OpenFlow match (one with no OXM TLVs) matches every packet. Match fields that should be wildcarded are omitted from the OpenFlow match.		Y	
7.2.2.5		Flow Match Field Masking	The masks are defined such that a 0 in a given bit position indicates a \don't care" match for the same bit in the corresponding field, whereas a 1 means match the bit exactly.		Y	Some limitation, please see the configuration guide.
7.2.2.6		Flow Match Field Prerequisite	In general, matching header fields of a protocol can only be done if the OpenFlow match explitly matches the corresponding protocol.		Y	
7.2.2.7		Flow Match Fields	Match fields contains: OFPXMT_OFB_IN_PORT, OFPXMT_OFB_IN_PHY_PORT,		Y	
		OXM_OF_IN_PORT	/* Switch input port. */		Y	
		OXM_OF_IN_PHY_PORT	/* Switch physical input port. */	O		
		OXM_OF_METADATA	/* Metadata passed between tables. */	O		
		OXM_OF_ETH_DST	/* Ethernet destination address. */		Y	
		OXM_OF_ETH_SRC	/* Ethernet source address. */		Y	
		OXM_OF_ETH_TYPE	/* Ethernet frame type. */		Y	
		OXM_OF_VLAN_VID	/* VLAN id. */	O	Y	
		OXM_OF_VLAN_PCP	/* VLAN priority. */	O	Y	
		OXM_OF_IP_DSCP	/* IP DSCP (6 bits in ToS field). */	O	Y	
		OXM_OF_IP_ECN	/* IP ECN (2 bits in ToS field). */	O	N	
		OXM_OF_IP_PROTO	/* IP protocol. */		Y	
		OXM_OF_IPV4_SRC	/* IPv4 source address. */		Y	
		OXM_OF_IPV4_DST	/* IPv4 destination address. */		Y	
		OXM_OF_TCP_SRC	/* TCP source port. */		Y	
		OXM_OF_TCP_DST	/* TCP destination port. */		Y	
		OXM_OF_UDP_SRC	/* UDP source port. */		Y	
		OXM_OF_UDP_DST	/* UDP destination port. */		Y	
		OXM_OF_SCTP_SRC	/* SCTP source port. */	O	N	
		OXM_OF_SCTP_DST	/* SCTP destination port. */	O	N	
		OXM_OF_ICMPV4_TYPE	/* ICMP type. */	O	Y	
		OXM_OF_ICMPV4_CODE	/* ICMP code. */	O	Y	
		OXM_OF_ARP_OP	/* ARP opcode. */	O	Y	
		OXM_OF_ARP_SPA	/* ARP source IPv4 address. */	O	Y	
		OXM_OF_ARP_TPA	/* ARP target IPv4 address. */	O	Y	
		OXM_OF_ARP_SHA	/* ARP source hardware address. */	O	N	
		OXM_OF_ARP_THA	/* ARP target hardware address. */	O	N	
		OXM_OF_IPV6_SRC	/* IPv6 source address. */		Y	
		OXM_OF_IPV6_DST	/* IPv6 destination address. */		Y	
		OXM_OF_IPV6_FLABEL	/* IPv6 Flow Label */	O	N	
		OXM_OF_ICMPV6_TYPE	/* ICMPv6 type. */	O	N	
		OXM_OF_ICMPV6_CODE	/* ICMPv6 code. */	O	N	
		OXM_OF_IPV6_ND_TARGET	/* Target address for ND. */	O	N	
		OXM_OF_IPV6_ND_SLL	/* Source link-layer for ND. */	O	N	
		OXM_OF_IPV6_ND_TLL	/* Target link-layer for ND. */	O	N	
		OXM_OF_MPLS_LABEL	/* MPLS label. */	O	N	

		OXM_OF_MPLS_TC	/* MPLS TC. */	O	N	
7.2.2.8		Experimenter Flow Match Fields	Experimenter-specific ow match fields,may be defined using the oxm_class=OFPXMC_EXPERIMENTER	O	N	
7.2.3		Flow Instruction Structures	Flow instructions associated with a flow table entry are executed when a flow matches the entry.			
7.2.4		Action Structures				
		OFPAT_OUTPUT = 0,	/* Output to switch port. */		Y	
		OFPAT_COPY_TTL_OUT = 11,	/* Copy TTL "outwards" -- from next-to-outermost to outermost */		Y	
		OFPAT_COPY_TTL_IN = 12,	/* Copy TTL "inwards" -- from outermost to next-to-outermost */		Y	
		OFPAT_SET_MPLS_TTL = 15,	/* MPLS TTL */		Y	
		OFPAT_DEC_MPLS_TTL = 16,	/* Decrement MPLS TTL */		N	
		OFPAT_PUSH_VLAN = 17,	/* Push a new VLAN tag */		Y	
		OFPAT_POP_VLAN = 18,	/* Pop the outer VLAN tag */		Y	
		OFPAT_PUSH_MPLS = 19,	/* Push a new MPLS tag */		Y	
		OFPAT_POP_MPLS = 20,	/* Pop the outer MPLS tag */		Y	
		OFPAT_SET_QUEUE = 21,	/* Set queue id when outputting to a port */		Y	
		OFPAT_GROUP = 22,	/* Apply group. */		Y	
		OFPAT_SET_NW_TTL = 23,	/* IP TTL. */		N	
		OFPAT_DEC_NW_TTL = 24,	/* Decrement IP TTL. */		N	
		OFPAT_SET_FIELD = 25,	/* Set a header field using OXM TLV format. */		Y	
		OFPAT_PUSH_PBB = 26	/* Push a new PBB service tag (I-TAG) */		Y	
		OFPAT_POP_PBB = 27	/* Pop the outer PBB service tag (I-TAG) */		Y	
		OFPAT_EXPERIMENTER = 0xffff			N	
7.2.5		Experimenter Structure	Experimenter extensions provide a standard way for OpenFlow switches to offer additional functionality within the OpenFlow message type space.		N	
7.3	Controller-to-Switch Messages					
7.3.1		Handshake	The OFPT_FEATURES_REQUEST message is used by the controller to identify the switch and read its basic capabilities.		Y	
7.3.2		Switch Configuration	The controller is able to set and query configuration parameters in the switch with the OFPT_SET_CONFIG and and OFPT_GET_CONFIG_REQUEST messages, respectively.		Y	
7.3.3		Flow Table Configuration	Flow entries are modified in the flow table using the OFP_FLOW_MOD request.		Y	
7.3.4		Modify State Messages			Y	
7.3.4.1		Modify Flow Table Message	The controller can configure the dynamic state in a flow table with the OFP_TABLE_MOD request.		Y	
7.3.4.2		Modify Flow Entry Message	Modifications to a flow table from the controller are done with the OFPT_FLOW_MOD message.		Y	
7.3.4.3		Modify Group Entry Message	Modifications to the group table from the controller are done with the OFPT_GROUP_MOD message.		Y	
7.3.4.4		Port Modification Message	The controller uses the OFPT_PORT_MOD message to modify the behavior of the port.		Y	
7.3.4.5		Meter Modification Messages	Modifications to a meter from the controller are done with the OFPT_METER_MOD message.		Y	
7.3.5		Multipart Messages	Multipart messages are used to encode requests or replies that potentially carry a large amount of dataand would not always fit in a single OpenFlow message, which is limited to 64KB.			
7.3.5.1		Description	Information about the switch manufacturer, hardware revision, software revision, serial number, and		Y	

			adescription field is available from the OFPMP_DESC multipart request type.			
7.3.5.2		Individual Flow Statistics	Information about individual flow entries is requested with the OFPMP_FLOW multipart request type.		Y	
7.3.5.3		Aggregate Flow Statistics	Aggregate information about multiple flow entries is requested with the OFPMP_AGGREGATE multipart request type.		Y	
7.3.5.4		able Statistics	Information about tables is requested with the OFPMP_TABLE multipart request type.		Y	
7.3.5.5		Table Description	The OFPMP_TABLE_DESC multipart request message provides a way to list the current configuration of the tables on a switch, which is set using the OFPT_TABLE_MOD message.		Y	
7.3.5.6		Table Features	The OFPMP_TABLE_FEATURES multipart type allows a controller to both query for the capabilities of existing tables, and to optionally ask the switch to reconfigure its tables to match a supplied configuration.		N	
		Table Features request and reply	If the OFPMP_TABLE_FEATURES request body is empty the switch will return an array of struct ofp_table_features containing the capabilities of the currently configured flow tables.		N	
		Table Features properties	A property definition contains the property type, length, and any associated data.		N	
7.3.5.7		Port Statistics	Information about ports statistics is requested with the OFPMP_PORT_STATS multipart request type.		Y	
7.3.5.8		Port Description	The port description request OFPMP_PORT_DESCRIPTION enables the controller to get a description of all the ports in the system that support OpenFlow.		Y	
7.3.5.9		Queue Statistics	The OFPMP_QUEUE_STATS multipart request message provides queue statistics for one or more ports and one or more queues.		N	
7.3.5.10		Queue Descriptions	The controller can query the switch for configured queues on a port using OFPMP_QUEUE_DESC multipart request.		Y	
7.3.5.11		Group Statistics	The OFPMP_GROUP multipart request message provides statistics for one or more groups.		Y	
7.3.5.12		Group Description	The OFPMP_GROUP_DESC multipart request message provides a way to list the set of groups on a switch along with their corresponding bucket actions.		Y	
7.3.5.13		Group Features	The OFPMP_GROUP_FEATURES multipart request message provides a way to list the capabilities of groups on a switch.		Y	
7.3.5.14		Meter Statistics	The OFPMT_METER stats request message provides statistics for one or more meters.		Y	
7.3.5.15		Meter Configuration Statistics	The OFPMT_METER_CONFIG stats request message provides configuration for one or more meter.		Y	
7.3.5.16		Meter Features Statistics	The OFPMT_METER_FEATURES stats request message provides the set of features of the metering subsystem.		Y	
7.3.5.17		Flow monitoring	The OFPMP_FLOW_MONITOR multipart type allows a controller to manage flow monitors, that keep track of changes to the flow tables.		N	
		Flow monitoring request	Flow monitor configuration is done with a OFPMP_FLOW_MONITOR multipart request		N	
		Flow monitoring reply	When the switch received a OFPMP_FLOW_MONITOR multipart request, it replies to it using a OFPMP_FLOW_MONITOR multipart reply, the transaction id (xid) of this reply must be the same as the request.		N	
		Flow monitoring pause	OpenFlow messages for flow monitor notifications can over flow the buffer space available to the switch either temporarily or more permanently.		N	
7.3.5.18		Experimenter Multipart	Experimenter-specific multipart messages are requested with the OFPMP_EXPERIMENTER multipart type.		N	

7.3.6		Packet-Out Message	When the controller wishes to send a packet out through the datapath, it uses the OFPT_PACKET_OUT message.		Y	
7.3.7		Barrier Message	When the controller wants to ensure message dependencies have been met or wants to receive notifications for completed operations, it may use an OFPT_BARRIER_REQUEST message.		Y	
7.3.8		Role Request Message	When the controller wants to change its role, it uses the OFPT_ROLE_REQUEST message.		Y	
7.3.9		Bundle messages				
7.3.9.1		Bundle control messages	The controller can create, destroy and commit bundles with the OFPT_BUNDLE_CONTROL request.		Y	
7.3.9.2		Bundle Add message	The controller can add requests to a bundle using the OFPT_BUNDLE_ADD_MESSAGE message.		Y	
7.3.9.3		Bundle flags	Bundle flags enable to modify the behavior of a bundle.		Y	
7.3.9.4		Bundle properties	A property definition contains the property type, length, and any associated data.		Y	
7.3.9.5		Creating and opening a bundle	To create a bundle, the controller sends a OFPT_BUNDLE_CONTROL message with type OFPBCT_OPEN_REQUEST.		Y	
7.3.9.6		Adding messages to a bundle	The switch adds message to a bundle using the OFPT_BUNDLE_ADD_MESSAGE.		Y	
7.3.9.7		Closing a bundle	To finish recording a bundle, the controller may sends a OFPT_BUNDLE_CONTROL message with type OFPBCT_CLOSE_REQUEST.		Y	
7.3.9.8		Committing Bundles	To finish and apply the bundle, the controller sends a OFPT_BUNDLE_CONTROL message with type OFPBCT_COMMIT_REQUEST.		Y	
7.3.9.9		Discarding Bundles	To finish and discard the bundle, the controller sends a OFPT_BUNDLE_CONTROL message with type OFPBCT_DISCARD_REQUEST.		Y	
7.3.9.10		Other bundle error conditions	If a OFPT_BUNDLE_CONTROL message contains an invalid type, the switch must reject the request and send an ofp_error_msg with OFPET_BUNDLE_FAILED type and OFPBFC_BAD_TYPE code.		N	
7.3.10		Set Asynchronous Configuration Message	The switch manages a per-controller asynchronous configuration, which defines the asynchronous messages that it wants to receive (other than error messages) on a given OpenFlow channel.		Y	
7.4	Asynchronous Messages					
7.4.1		Packet-In Message	When packets are received by the datapath and sent to the controller, they use the OFPT_PACKET_IN.		Y	
7.4.2		Flow Removed Message	If the controller has requested to be notified when flow entries time out or are deleted from table, the data path does this with the OFPT_FLOW_REMOVED message.		Y	
7.4.3		Port Status Message	As ports are added, modified, and removed from the datapath, the controller needs to be informed with the OFPT_PORT_STATUS message		Y	
7.4.4		Controller Role Status Message	When a controller has its role changed by the switch, and not directly changed by that controller using a OFPT_ROLE_REQUEST message, the corresponding controller must be informed with a OFPT_ROLE_STATUS message.		Y	
7.4.5		Table Status Message	When the table state changes, the controller needs to be informed with the OFPT_TABLE_STATUS message.		Y	
7.4.6		Request Forward Message	When a controller modifies the state a groups and meters, the request that successfully modifies this state may be forwarded to other controller.		Y	
7.5	Symmetric Messages					
7.5.1		Hello	The OFPT_HELLO message consists of an OpenFlow header plus a set of variable size hello elements.		Y	
7.5.2		Echo Request	An Echo Request message consists of an OpenFlow header plus an arbitrary-length data field.		Y	

7.5.3		Echo Reply	An Echo Reply message consists of an OpenFlow header plus the unmodified data field of an echo request message.		Y	
7.5.4		Error Message	Error messages are used by the switch or the controller to notify the other side of the connection of problems.		Y	
7.5.5		Experimenter Message			N	
A	Header file openflow.h					
B	Release Notes					
B.14	OpenFlow version 1.4.0					
B.14.1		More extensible wire protocol			N	
B.14.2		More descriptive reasons for packet-in			Y	
B.14.3		Optical port properties			N	
B.14.4		Flow-removed reason for meter delete.			Y	
B.14.5		Flow monitoring			N	
B.14.6		Role status events			Y	
B.14.7		Eviction			Y	
B.14.8		Vacancy events			Y	
B.14.9		Bundles			Y	
B.14.10		Synchronized tables			N	
B.14.11		Group and Meter change notifications			Y	
B.14.12		Error code for bad priority			N	
B.14.13		Error code for Set-async-config			Y	
B.14.14		PBB UCA header field			N	
B.14.15		Error code for duplicate instruction			Y	
B.14.16		Error code for multipart timeout			Y	
B.14.17		Change default TCP port to 6653			N	

PicOS Support for OpenFlow 1.4.0

OpenFlow is a communication protocol used in software-defined networking (SDN). It enables an SDN controller to communicate instructions to the forwarding plane of network switches and routers, including virtual switches and routers. Using OpenFlow, the SDN controller can make changes to the switch and router flow tables, enabling administrators to quickly make network changes such as to optimize network performance or test new configurations. OpenFlow is intended to be an extensible protocol, enabling SDN programmers to define additional elements, such as actions or port properties that address new network technologies as they emerge. OpenFlow is maintained by the Open Network Foundation's Open Datapath project, which is seeking to build a foundation for a rich SDN ecosystem and software development lifecycle. The Pica8 PICOS network operating system supports OpenFlow.

This document contains OpenFlow 1.4.0 features supported by the Pica8 PICOS software. For clarity, the feature names in this table are identical to the feature names found in OpenFlow Switch Specification, Version 1.4.0.

OpenFlow Messages

Each OpenFlow message begins with the OpenFlow header. The OpenFlow header has several fields, including the **type** field. The **type** field identifies the type of OpenFlow message.

The OpenFlow protocol has three message types: *symmetric*, *controller-to-switch*, and *asynchronous*. Each message type has multiple sub-types.

Symmetric Messages

Symmetric messages are unsolicited messages that may be initiated by either the switch or the controller. Symmetric messages are sent without explicit solicitation in either direction. The following table describes PicOS support for symmetric messages:

Table 1 PicOS Support for OpenFlow Symmetric Messages

Message	Support	Comments
OFPT_HELLO	Supported	
OFPT_ERROR	Supported	
OFPT_ECHO_REQUEST	Supported	
OFPT_ECHO_REPLY	Supported	
OFPT_EXPERIMENTER	Not Supported	

Controller-to-Switch Messages

As the title suggests, Controller-to-switch messages are sent from the controller to the switch. These messages are used to directly manage the state of a switch. Controller-to-switch messages may or may not require a response from the switch.

The following table describes PicOS support for controller-to-switch messages:

Table 2 PicOS Support for OpenFlow Controller-to-Switch Messages

Message	Support	Comments
OFPT_FEATURES_REQUEST	Supported	
OFPT_FEATURES_REPLY See Capabilities Supported by Datapath		
OFPT_GET_CONFIG_REQUEST	Supported	
OFPT_GET_CONFIG_REPLY		
OFPT_SET_CONFIG	Supported	
OFPT_PACKET_OUT	Supported	
OFPT_FLOW_MOD	Supported	
OFPT_GROUP_MOD	Supported	
OFPT_PORT_MOD	Supported	
OFPT_TABLE_MOD	Supported	
OFPT_MULTIPART_REQUEST See Multipart Messages	Supported	
OFPT_MULTIPART_REPLY See Multipart Messages	Supported	
OFPT_BARRIER_REQUEST	Supported	

Message	Support	Comments
OFPT_BARRIER_REPLY		
OFPT_ROLE_REQUEST	Supported	
OFPT_ROLE_REPLY		
OFPT_GET_ASYNC_REQUEST	Supported	
OFPT_GET_ASYNC_REPLY	Supported	
OFPT_SET_ASYNC	Supported	
OFPT_METER_MOD	Supported	

Asynchronous Messages

Asynchronous messages are sent from the switch to the controller. These messages are used to communicate network events and switch state changes to the controller. Asychronous messages are sent without a controller explicitly requesting them from a switch.

The following table describes PicOS support for asynchronous messages:

Table 3 PicOS Support for OpenFlow Asynchronous Messages

Message	Support	Comments
OFPT_PACKET_IN	Supported	
OFPT_FLOW_REMOVED	Supported	
OFPT_PORT_STATUS	Supported	
OFPT_ROLE_STATUS	Supported	
OFPT_TABLE_STATUS	Supported	
OFPT_REQUESTFORWARD		

Bundle Operations

The following table describes PicOS support for bundle operations:

Table 4 PicOS Support for OpenFlow Bundle Operations

Message	Support	Comments
OFPT_BUNDLE_CONTROL	Supported	
OFPT_BUNDLE_ADD_MESSAGE	Supported	

Multipart Messages

The following table describes PicOS support for multipart messages: a single OpenFlow message cannot be larger than 64 kilobytes. Multipart messages are used to encode requests or replies that would carry a large amount of data, and would not always fit in a single OpenFlow message. The sender encodes the request or reply as a sequence of multipart messages with a specific multipart type. The receiver re-assembles the request or reply.

Table 5 PicOS Support for OpenFlow Multipart Messages

Message	Support	Comments
OFPMP_DESC	Supported	
OFPMP_FLOW	Supported	
OFPMP_TABLE	Supported	
OFPMP_TABLE_DESC	Supported	
OFPMP_TABLE_FEATURES	Supported	
OFPMP_PORT_STATS	Supported	
OFPMP_PORT_DESCRIPTION	Supported	
OFPMP_QUEUE_STATS	Not Supported	
OFPMP_QUEUE_DESC	Supported	
OFPMP_GROUP	Supported	
OFPMP_GROUP_DESC	Supported	

Message	Support	Comments
OFPMP_GROUP_FEATURES	Supported	
OFPMT_METER	Supported	
OFPMT_METER_CONFIG	Supported	
OFPMT_METER_FEATURES	Supported	
OFPMP_FLOW_MONITOR	Supported	
OFPMP_EXPERIMENTER	Not Supported	

Capabilities Supported by Datapath

The controller sends an **OFPT_FEATURES_REQUEST** message to the switch once a session is established. The switch responds to the **OFPT_FEATURES_REQUEST** message with an **OFPT_FEATURES_REPLY** message. The **OFPT_FEATURES_REPLY** message has several fields, including the **capabilities** field. The **capabilities** field identifies the capabilities supported by the switch datapath.

The **capabilties** field is a combination of the following bits/flags:

Table 6 PicOS Support for OpenFlow Capabilities Supported by Datapath

Specification	Support	Comments
OFPC_FLOW_STATS	Supported	
OFPC_TABLE_STATS	Supported	
OFPC_PORT_STATS	Supported	
OFPC_GROUP_STATS	Supported	
OFPC_IP_REASM		
OFPC_QUEUE_STATS		
OFPC_PORT_BLOCKED		

OpenFlow Ports

OpenFlow ports are abstract network interfaces used for passing traffic between the OpenFlow switch and the rest of the network. An OpenFlow switch makes a number of OpenFlow ports available. The set of OpenFlow ports does not have to be identical to the set of physical network interfaces on the switch hardware.

Port Descriptions

The OpenFlow switch receives and sends packets on OpenFlow ports. The switch may define physical and logical ports. OpenFlow specification also defines some reserved ports.

Table 7 PicOS Support for OpenFlow Ports

Specification	Support	Comments
OFPP_MAX		
OFPP_IN_PORT	Supported	
OFPP_TABLE	Supported	
OFPP_NORMAL	Supported	
OFPP_FLOOD	Supported	
OFPP_ALL	Supported	
OFPP_CONTROLLER	Supported	
OFPP_LOCAL	Supported	
OFPP_ANY	Supported	

Port Administrative Settings

The following table describes PicOS support for administrative settings of OpenFlow ports:

Table 8 PicOS Support for OpenFlow Port Administrative Settings

Specification	Support	Comments
OFPPC_PORT_DOWN	Supported	
OFPPC_NO_RECV		

Specification	Support	Comments
OFPPC_NO_FWD		
OFPPC_NO_PACKET_IN		

Port States

The following table describes PicOS support for OpenFlow port states:

Table 9 PicOS Support for OpenFlow Port States

Specification	Support	Comments
OFPPS_LINK_DOWN	Supported	
OFPPS_BLOCKED		
OFPPS_LIVE		

Port Features

The following table describes PicOS support for OpenFlow port features available in the datapath:

Table 10 PicOS Support for OpenFlow Port Features

Specification	Support	Comments
OFPPF_10MB_HD		
OFPPF_10MB_FD	Supported	
OFPPF_100MB_HD		
OFPPF_100MB_FD	Supported	
OFPPF_1GB_HD		
OFPPF_1GB_FD	Supported	
OFPPF_10GB_FD	Supported	
OFPPF_40GB_FD	Supported	
OFPPF_100GB_FD	Supported	
OFPPF_1TB_FD		
OFPPF_OTHER		
OFPPF_COPPER	Supported	
OFPPF_FIBER	Supported	
OFPPF_AUTONEG	Supported	
OFPPF_PAUSE	Supported	
OFPPF_PAUSE_ASYM		

OpenFlow Instructions

Each flow entry contains a set of instructions that are executed to match a packet to an entry. The following table details OpenFlow instructions supported by PicOS:

Table 11 PicOS Support for OpenFlow Instructions

Specification	Support	Comments
OFPIT_GOTO_TABLE	Supported	only next-table-id; is executed last.
OFPIT_WRITE_METADATA	Supported	
OFPIT_WRITE_ACTIONS	Supported	
OFPIT_APPLY_ACTIONS	Supported	
OFPIT_CLEAR_ACTIONS	Supported	
OFPIT_METER	Supported	
OFPIT_EXPERIMENTER		

OpenFlow Action Types

The following table details OpenFlow action types supported by PicOS:

Table 12 PicOS Support for OpenFlow Action Types

Specification	Support	Comments
OFPAT_OUTPUT	Supported	
OFPAT_COPY_TTL_OUT	Supported	
OFPAT_COPY_TTL_IN	Supported	
OFPAT_SET_MPLS_TTL	Supported	
OFPAT_DEC_MPLS_TTL	Not Supported	
OFPAT_PUSH_VLAN	Supported	
OFPAT_POP_VLAN	Supported	
OFPAT_PUSH_MPLS	Supported	
OFPAT_POP_MPLS	Supported	
OFPAT_SET_QUEUE	Supported	
OFPAT_GROUP	Supported	
OFPAT_SET_NW_TTL	Not Supported	
OFPAT_DEC_NW_TTL	Not Supported	
OFPAT_SET_FIELD	Supported	
OFPAT_PUSH_PBB	Supported	
OFPAT_POP_PBB	Supported	
OFPAT_EXPERIMENTER	Not Supported	

OpenFlow Match Fields

A match field may include the packet header, the ingress port, and the metadata value. A match field may use wildcards to match any value and, in some cases, bitmasks. A packet is matched against a match field.

The following table details the OXM flow match field types supported by PicOS:

Table 13 PicOS Support for OpenFlow Flow Match Fields

Specification	Support	Comments
OFPXMT_OFB_IN_PORT	Supported	
OFPXMT_OFB_IN_PHY_PORT	Supported	
OFPXMT_OFB_METADATA		
OFPXMT_OFB_ETH_DST	Supported	
OFPXMT_OFB_ETH_SRC	Supported	
OFPXMT_OFB_ETH_TYPE	Supported	
OFPXMT_OFB_VLAN_VID	Supported	
OFPXMT_OFB_VLAN_PCP	Supported	
OFPXMT_OFB_IP_DSCP	Supported	
OFPXMT_OFB_IP_ECN		
OFPXMT_OFB_IP_PROTO	Supported	
OFPXMT_OFB_IPV4_SRC	Supported	
OFPXMT_OFB_IPV4_DST	Supported	
OFPXMT_OFB_TCP_SRC	Supported	
OFPXMT_OFB_TCP_DST	Supported	
OFPXMT_OFB_UDP_SRC	Supported	
OFPXMT_OFB_UDP_DST	Supported	
OFPXMT_OFB_SCTP_SRC		

Specification	Support	Comments
OFPXMT_OFB_SCTP_DST		
OFPXMT_OFB_ICMPV4_TYPE	Supported	
OFPXMT_OFB_ICMPV4_CODE	Supported	
OFPXMT_OFB_ARP_OP	Supported	
OFPXMT_OFB_ARP_SPA	Supported	
OFPXMT_OFB_ARP_TPA	Supported	
OFPXMT_OFB_ARP_SHA		
OFPXMT_OFB_ARP_THA		
OFPXMT_OFB_IPV6_SRC	Supported	
OFPXMT_OFB_IPV6_DST	Supported	
OFPXMT_OFB_IPV6_FLABEL	Supported	
OFPXMT_OFB_ICMPV6_TYPE		
OFPXMT_OFB_ICMPV6_CODE		
OFPXMT_OFB_IPV6_ND_TARGET		
OFPXMT_OFB_IPV6_ND_SLL		
OFPXMT_OFB_IPV6_ND_TLL		
OFPXMT_OFB_MPLS_LABEL		
OFPXMT_OFB_MPLS_TC		
OFPXMT_OFP_MPLS_BOS		
OFPXMT_OFB_PBB_ISID	Supported	
OFPXMT_OFB_TUNNEL_ID	Supported	
OFPXMT_OFB_IPV6_EXTHDR		
OFPXMT_OFB_PBB_UCA		

OpenFlow Group Types

The following table describes PicOS support for OpenFlow group types:

Table 14 PicOS Support for OpenFlow Group Types

Specification	Support	Comments
OFPGT_ALL	Supported	
OFPGT_SELECT	Supported	
OFPGT_INDIRECT	Supported	
OFPGT_FF	Supported	

Introduction to Open vSwitch

Open vSwitch, sometimes abbreviated as OVS, is an open-source multilayer virtual switch. Open vSwitch can operate both as a soft switch running within the hypervisor and as the control stack for switching silicon. Learn more about Open vSwitch here.

Open vSwitch is already included in the Pica8 PicOS software and runs as a process in PicOS.

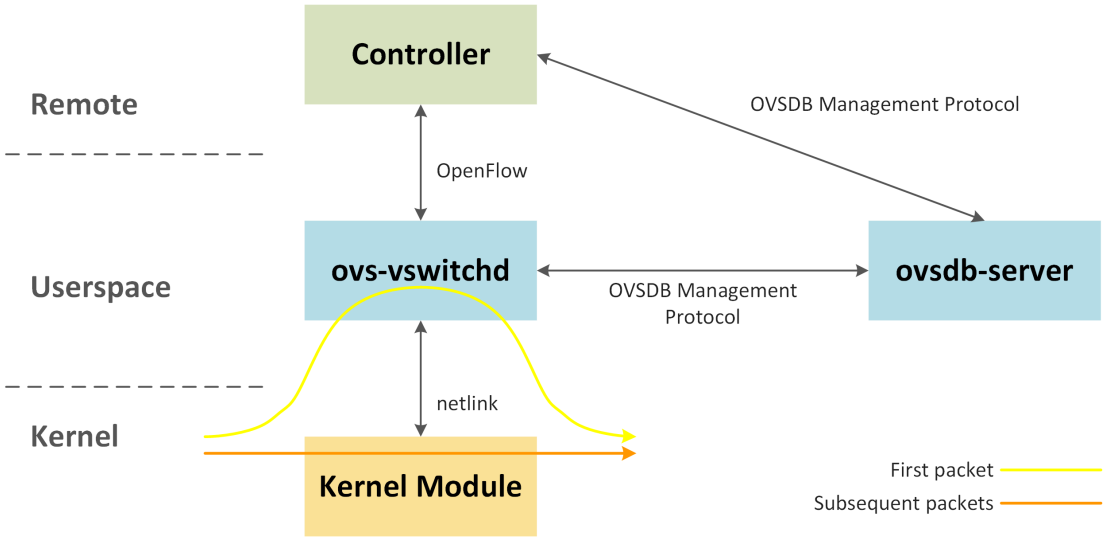
The Open vSwitch version available on a PicOS switch can be determined using the **ovs-appctl version** command from the Linux shell.

```
admin@Switch$ovs-appctl version
ovs-vswitchd (Open vSwitch) 2.3.0
Compiled May 24 2015 21:37:14
```

Open vSwitch Components

The main components of Open vSwitch are:

1. Kernel Module
2. Open vSwitch Database
3. Open vSwitch Daemon



Kernel Module

Kernel modules are pieces of code that can be loaded and unloaded into the kernel on demand. They extend the functionality of the kernel without having to reboot the system. Without modules, new functionality would have to be added directly into the kernel image, resulting in monolithic, larger kernels.

The kernel module handles switching and tunneling. It is designed to be fast and simple. When a packet is received and a match is found, associated actions are executed and counters are updated. Otherwise, packets are sent to userspace.

To manage the kernel module, use the **ovs-dpctl** command-line tool.

Open vSwitch Database

The Open vSwitch Database (OVSDB) holds switch configuration including bridge, interface, and tunnel definitions. The OVSDB and OpenFlow controller addresses are also held by the OVSDB. The OVSDB, and hence switch configuration, is stored on persistent storage and survives a reboot.

The **ovsdb-server** communicates with **ovs-vswitchd** and the controller using the OVSDB management protocol, defined in RFC 7047.

To manage **ovsdb-server**, use the **ovsdb-tool** and **ovs-vsctl** command-line tools.

Open vSwitch Daemon

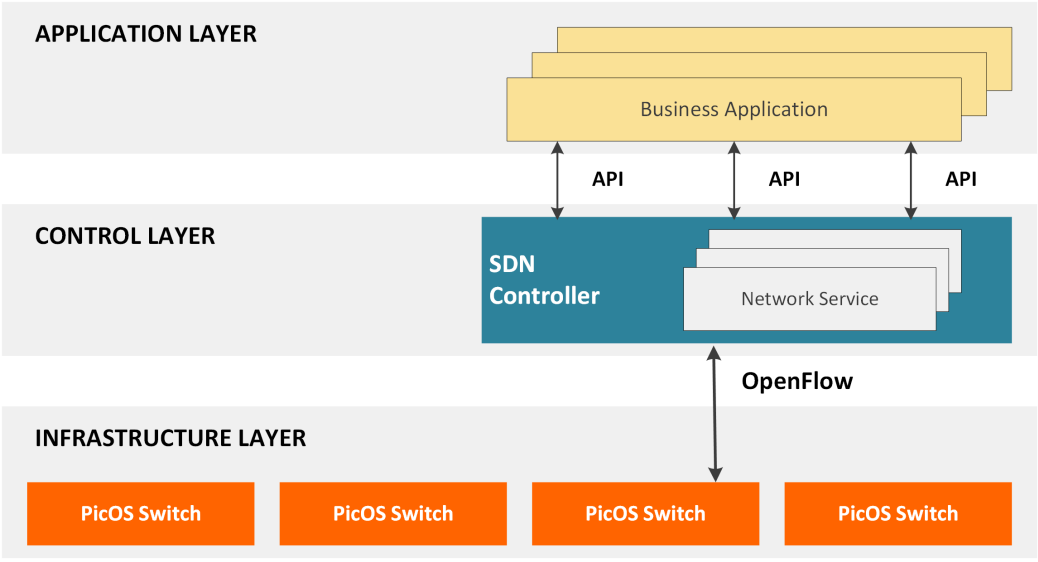
The Open vSwitch daemon (**ovs-vswitchd**) is the core component of an Open vSwitch incarnation. It communicates with the controller using OpenFlow. It communicates with the Open vSwitch Database Server (**ovsdb-server**) using the Open vSwitch Database (OVSDB) management protocol, defined in RFC 7047. The **ovs-vswitchd** communicates with the kernel module over netlink - a Linux kernel interface used for communication between userspace processes and the kernel.

The **ovs-vswitchd** supports multiple independent data paths, known as bridges.

To manage **ovs-vswtichd**, use the **ovs-ofctl** and **ovs-appctl** command-line tools.

Introduction to OpenFlow

The separation of control and data planes is one of the fundamental principles of SDN (Software-Defined Networking). OpenFlow is the first standard interface for communication between the control and data planes of an SDN architecture. The following graphic presents the role OpenFlow plays in the SDN framework:



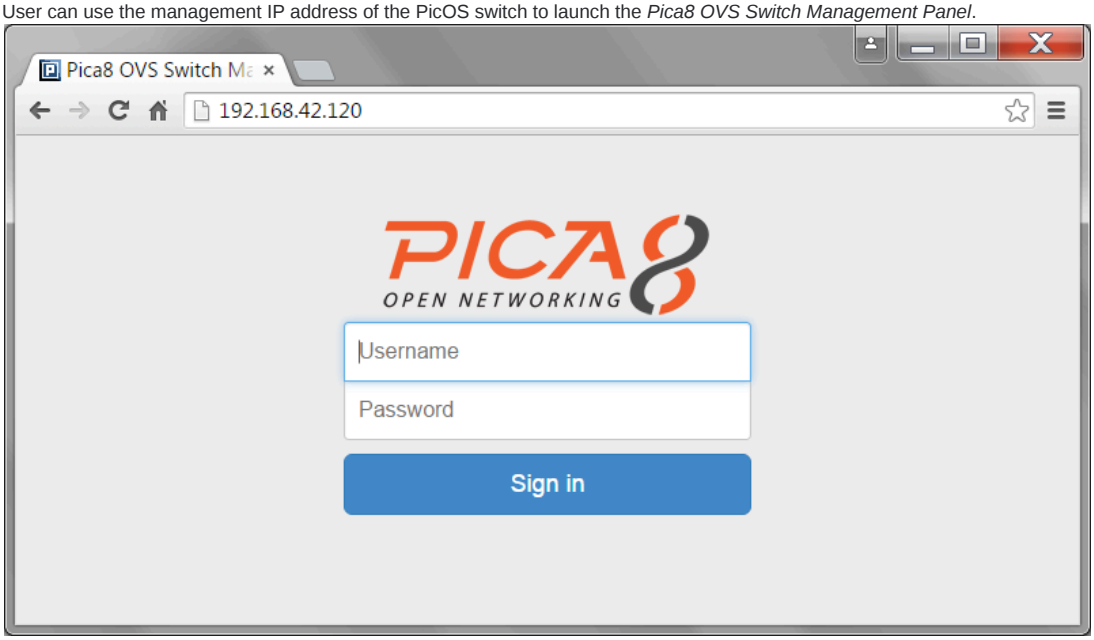
Learn more about OpenFlow here.

OVS Web User Interface

- Login Interface
- Monitoring the Switch
- Adding a Bridge
- Add a Port
- Add GRE Port
- Add Group Table
- Add or Edit a Controller
- Edit Flow Tables
- Edit Lag Interface

Login Interface

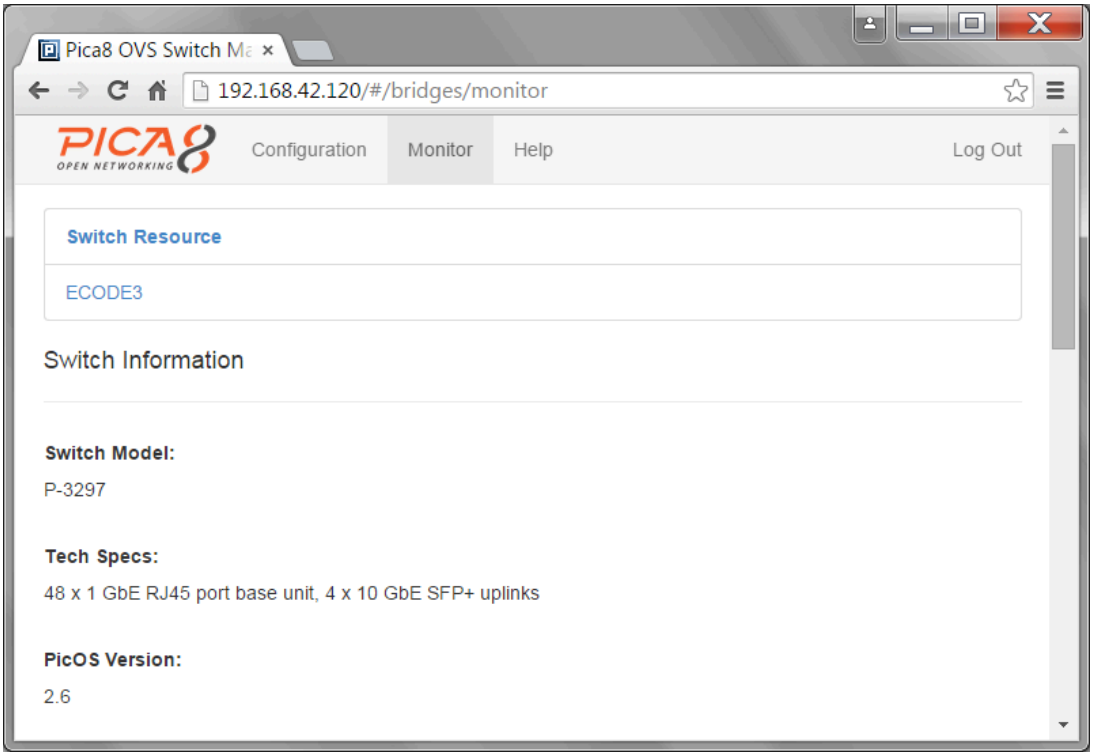
User can use the management IP address of the PicOS switch to launch the *Pica8 OVS Switch Management Panel*.



Monitoring the Switch

The **Monitor** tab provides provides basic switch information and allows users to monitor the switch operation.

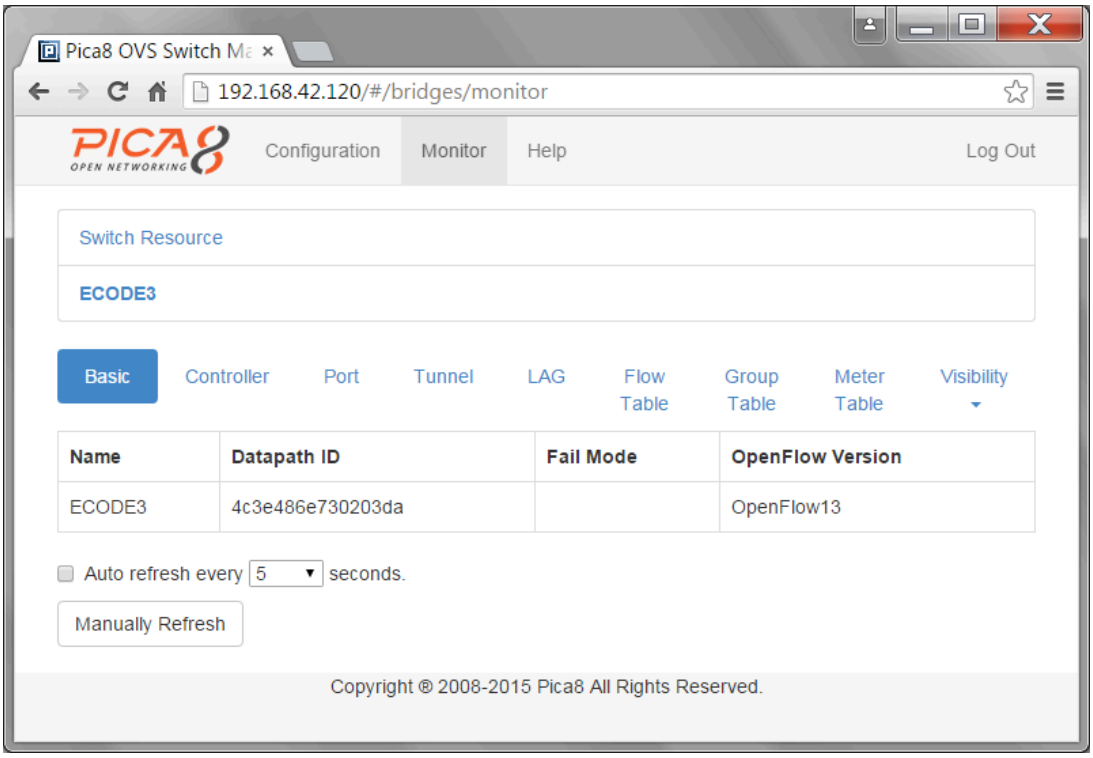
The **Monitor** tab may have several sections including the default *Switch Resource*, as shown below:



The default *Switch Resource* section, provides the following pieces of information:

- Switch Model
- Tech Specs
- PicOS Version
- Software Revision
- Web Interface Version
- Open vSwitch Version
- Maximum Flow Numbers
- Storage Capacity
- MAC Address
- IP Address
- Gateway
- OVSDB Config File Location
- CPU Load

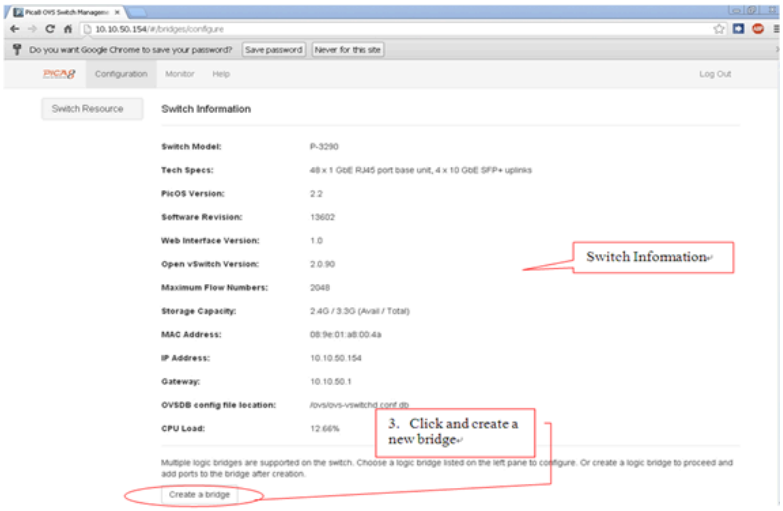
The **Monitor** tab also allows users to monitor any bridges created on the switch. The following screenshot displays information about a bridge that has been named *ECODE3*:



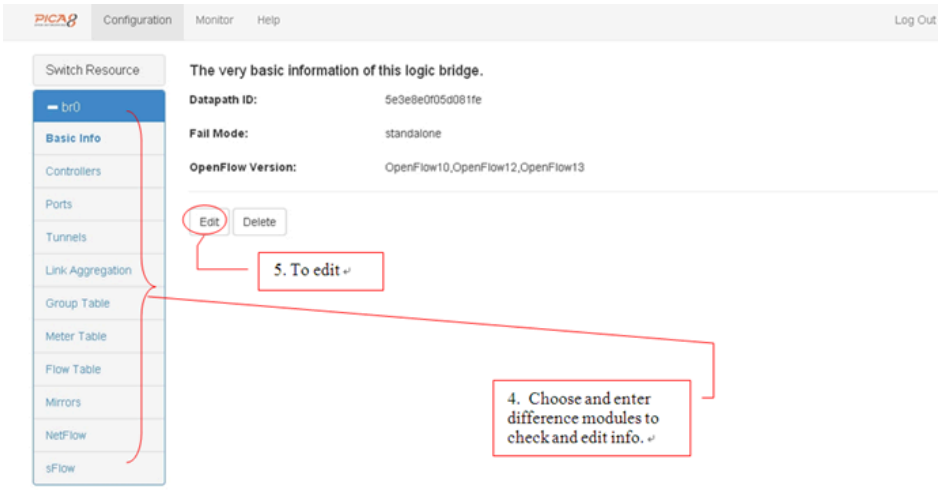
User can refresh bridge information manually or set it to auto-refresh at the specified interval.

Adding a Bridge

Once user has successfully launched the user interface, the ***Configuration*** tab reveals the switch resource section that provides basic switch information. To create a bridge, click on the ***Create a bridge*** icon.

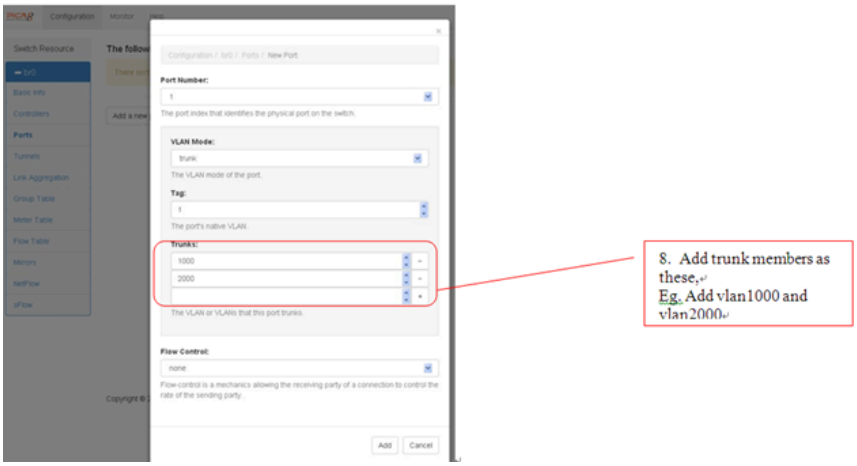


Once user has created a new bridge (br0 in example below), user can edit properties or delete it. The menu on the left (in the graphic below) allows users to view, edit, and change any of the modules listed in the menu.



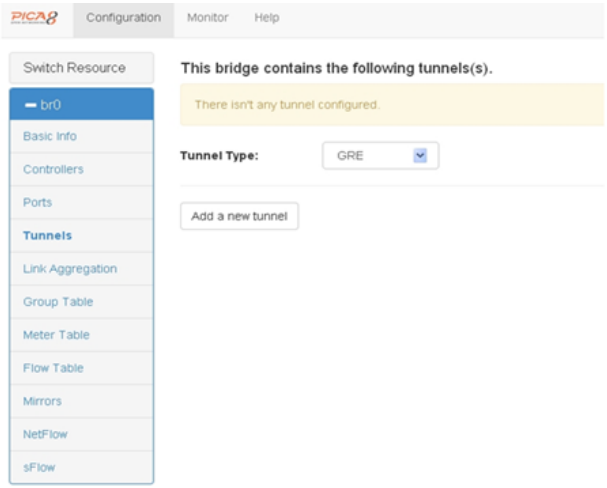
Add a Port

To add a new port, click on ***Port*** from the menu on the left of the screen. Complete the port number, VLAN mode, tag, and trunks. Then, click ***Add*** to save it.

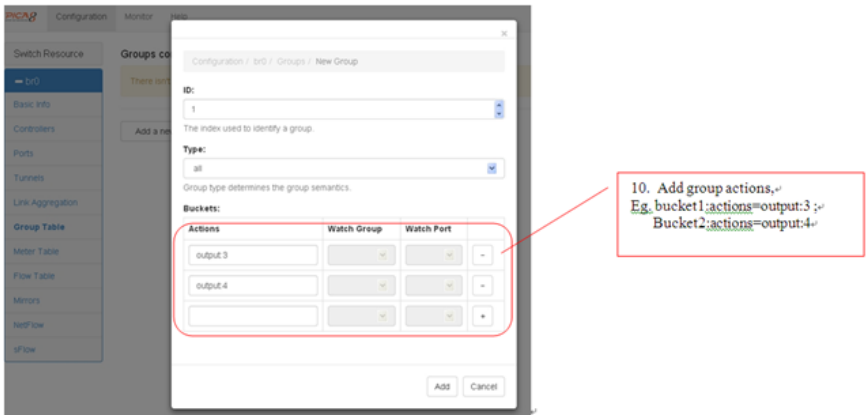


Add GRE Port

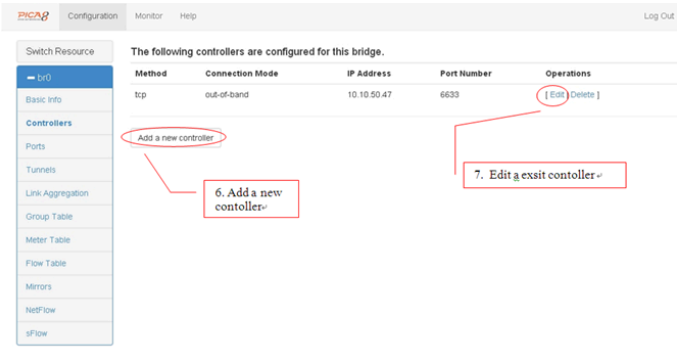
Select ***Tunnels*** from the menu to view the bridge's tunnel type or to add or edit a tunnel.



Add Group Table

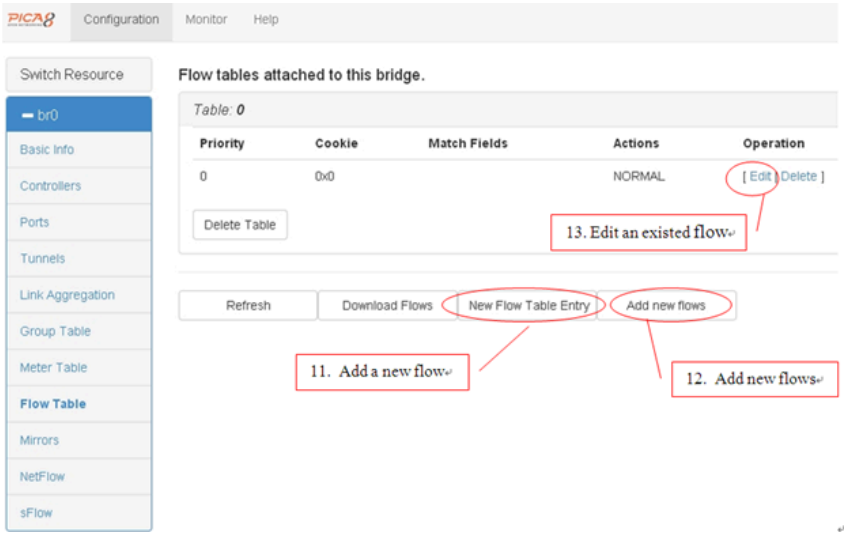


Add or Edit a Controller

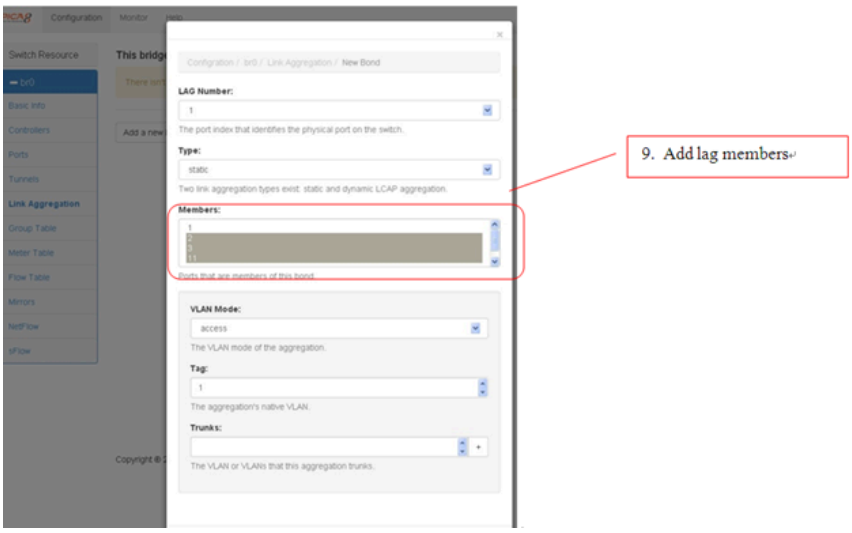


Edit Flow Tables

View the flow table attached to the bridge. Then, select required tabs to delete, edit, download, or add to the flow table.



Edit Lag Interface



Configuring Open vSwitch

Open vSwitch (also known as OVS), is an open source, multilayer virtual switch. It's designed to bring new levels of automation to networks through programmatic extensions and is used in many large production networks. Open vSwitch can be deployed as both a soft switch running on a hypervisor and as a control stack in switching silicon. It has been ported to various virtualization platforms and switching chipsets. It is the default switch in XenServer 6.0 and the Xen Cloud Platform, according to the Linux Foundation, which oversees the Open vSwitch project. It also supports Xen, KVM, Proxmox VE and VirtualBox. It supports standard management interfaces and protocols such as NetFlow, sFlow, IPFIX, RSPAN, CLI, LACP and 802.1ag.

Open vSwitch is included in the Pica8 PICOS network operating system, running as a process in PICOs. This document describes how to configure Open vSwitch in PICOS on an open white box switch.

- Basic Configuration in OVS Mode
- Configuring sFlow v5
- Configuring Port Mirroring
- OVSDB file
- OVS LLDP
- Enabling Radius in PicOS OVS Mode
- Inventory Database
- Broadcom Chip Limitation in OVS
  - Priority of Arp flow
  - Overlap flow
  - Vlan Isolation
  - ARP Flow in Combinated Mode Table
  - Limitations on trident3
- OVS CLI Enhancements
- Configuring Meter
- Configuration saving
- Configuring Buffer management
- Configuring snmp
- Configuring/Enabling SNMPv3
- Configuring Precision Time Protocol
- Configuring Tunneling
  - Configuring QinQ
  - Configuring MPLS
  - Configuring VXLAN
  - Configuring L2MPLS
  - Configuring L2GRE
  - Configuring PBB
  - Configuring GRE
  - Decapsulation by pop actions
- Configuring Bridge and Ports
  - Configuring Loopback
  - Configuring TPID in Port
  - Configuring ports in bridge
  - Configuring bridge
  - Configuring CDR
  - Configuring ovs Remotely
  - Configuring LFS
  - Configuring CFM
- Configuring LAG and LACP
  - Adding LAG and LACP
  - Symmetric Hashing in lag and ecmp
  - Lag hash
  - Lag Resilient hash
  - GTP hash
- Configuring QoS
  - WRED
  - CoS Mapping
  - Configuring QoS scheduler
  - Vlan Priority CoS Mapping
- Configuring Flow Table
  - Configuring egress flow table
  - Configuring udf flow
  - Configuring NAT flow
  - Optimizing TCAM Usage
  - Configuring Flow Handling Mode
  - Combinated Mode
  - Configuring TTP
  - Configuring option-match-vlan-type

    - Configuring Multi-Table
    - Configuring ECMP
    - Goto_table
    - VN-tag
- Configuring Group
    - Ecmp Select Group
    - LAG Select Group
    - Creating a Group Table
    - Mirror Group
- Configuring Controller or Manager
    - Connecting to a Controller
    - Creating SSL Connection to a Controller
    - Connecting to Manager
- Configuring Counter
    - Drop counter
    - Clear counter
    - Counter Interval
    - Port Counter Interval
- Switching Open vSwitch version
- Configuring rate limit
- Configuring IPv4/IPv6 address for management port
- Configuring the Duplex Mode of Optical Port
- Configuring Port Speed on AS9716-32D and N9550-32D

Basic Configuration in OVS Mode

This section describes the basic configuration of PicOS switches in OVS (Open vSwitch) mode.

Once users have access to the switch and have PicOS running in OVS mode, users need to configure the IP address and default gateway.

To configure the management IP address, users should use the **picos_boot** configuration script as described in PICOS Mode Selection. An alternative to using the configuration script is to manually edit the PicOS configuration file.

For accessing the switch through a user interface, instead of the management interface, some OpenFlow flows need to be configured to redirect management traffic to the control plane. This is needed only if the switch cannot be managed through the management interface.

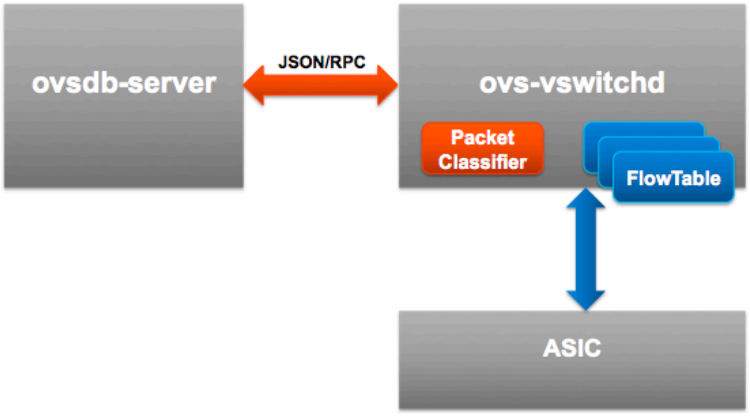
For example, users need to add the following flows to access the switch inband. The bridge **br0** has the MAC address *c8:0a:a9:04:49:19*.

```
root@PicOS-OVS#ovs-ofctl add-flow br0 priority=65300,in_port=local,dl_src=c8:0a:a9:04:49:19,actions=all
root@PicOS-OVS#ovs-ofctl add-flow br0 priority=65300,dl_dst=c8:0a:a9:04:49:19,actions=local
root@PicOS-OVS#ovs-ofctl add-flow br0 priority=65300,dl_dst=FF:FF:FF:FF:FF:FF,actions=all,local
```

Understanding OVS Components

The OVS as several components:

- **ovsdb-server:** A lightweight database server that provides switch level information (for example, information about switch ports).
- **ovs-vswitchd:** It is the core system component, which stores OpenFlow rules and performs flow based switching along with a companion Linux kernel module.
- **openvswitch_mod.ko:** It is a Linux kernel module doing most of the flow-based switching in PicOS OVS mode. This module is not loaded in the PicOS accelerated OVS, and is replaced by the ASIC (application-specific integrated circuit) for packet forwarding.
- **CLI:** The CLI (command-line interface) is used to control and manipulate other OVS components.



Understanding OVS CLI

The following three commands are used to control and monitor OVS:

- **ovs-vsctl Commands:** ovs-vsctl commands are used to control the **ovsdb-server** to create bridges, add interfaces, and configure interfaces.
- **ovs-appctl Commands:** ovs−appctl Commands are used to control the **ovs-vswitchd**.
- **ovs-ofctl Commands:** ovs−ofctl Commands are used to send OpenFlow queries. This can be used to manipulate the flows in **ovs-vswitchd**.

Each of those commands have a main page that can be viewed from the Linux shell on users' PicOS switch.

```
admin@Leaf1$man ovs-ofctl
ovs-ofctl(8)                Open vSwitch Manual                ovs-ofctl(8)
NAME
       ovs-ofctl - administer OpenFlow switches
SYNOPSIS
       ovs-ofctl [options] command [switch] [args...]
DESCRIPTION
       The  ovs-ofctl program is a command line tool for monitoring and admin-
       istering OpenFlow switches.  It can also show the current state  of  an
       OpenFlow  switch, including features, configuration, and table entries.
       It should work with any OpenFlow switch, not just Open vSwitch.
   OpenFlow Switch Management Commands
       These commands allow ovs-ofctl to monitor and  administer  an  OpenFlow
       switch.   It  is  able to show the current state of a switch, including
       features, configuration, and table entries.
```

```
       Most of these commands take an argument that specifies the  method  for
       connecting to an OpenFlow switch.  The following connection methods are
       supported:
<Some output omitted>
```

Configuring sFlow v5

PicOS OVS supports sFlow v5. User can configure the sFlow as follows:

```
root@PicOS-OVS$ ovs-vsctl  --id=@s create sFlow agent=eth0 target=\"10.10.50.207:9901\" header=128 sampling=5000 p
root@PicOS-OVS$
```

In the above example, the parameters are as follows:

```
COLLECTOR_IP=10.10.50.207
COLLECTOR_PORT=9901
AGENT_IP=eth0
HEADER_BYTES=128
SAMPLING_N=5000
POLLING_SECS=30
```

List the configuration of sflow:

```
root@PicOS-OVS$ovs-vsctl list sflow
_uuid               : 88d94294-4bb3-44f3-8a12-6055bf458de6
agent               : "eth0"
external_ids        : {}
header              : 128
polling             : 30
sampling            : 5000
targets             : ["10.10.50.207:9901"]
root@PicOS-OVS$
```

To delete an sFlow, use the clear command, as shown in the following example.:

```
root@PicOS-OVS$ ovs-vsctl -- clear Bridge br0 sflow
root@PicOS-OVS$
```

Tips

1.collector ip is ipv4 address,0.0.0.0 and 255.255.255.255 are invalid collector ip;

2.sample-rate equals to 0,no counter sample and flow sample packets,different with l2/l3 system;

polling-interval equals to 0,no counter sample packets,only flow sample packets.

sample-rate and polling-interval both equal to 0,no couter sample and flow sample packets.

3.header-len and sample rate do not have any limitations in ovs,while in l2/l3 system,header-len is [14,...1350] and sample rate is 0 or bigger than 100.

4.only support random sample mode.

5.Sample rate is 1,has some problem Bug 7939..This bug are related with port's line speed.I have some suggestion for this.

For 10G speed,500 is a better sample rate,at the same time，pps value is best to use 5；

For 1G speed,50 is a better sample rate,at the same time，pps value is best to use 5；

For 100M speed, 5 is the better sample rate,at the same time，pps value is best to use 5；

Configuring Port Mirroring

Chips mirror actions:

PRONTO3290 PRONTO3296 PRONTO3295(TR2)(egress mirror=true)
PRONTO3780 PRONTO3920 PRONTO3922 PRONTO3930 PRONTO3960 PRONTO3965 PRONTO3980 PRONTO3920 PRONTO3924(TD)

ES4654 AS4610_54P AS4610_54T AS4610_30P AS4610_30T(Helix4)(egress mirror=true)
PRONTO5101 PRONTO5401 AS6701_32X N2632XL N2948_6XL AS6712_32X AS5712_54X S4048 ARCTICA4806XP(TD2)

AS5812_54T AS5812_54X(TD2P)
DCS7032Q28 AS7712_32X Z9100 (TH)

Note：Egress mirror only works well on the platforms which egress mirror is true（eg:3290（Firebolt3），3296(Triumph2),4610 (helix4)).Otherwise the behaviour of egress mirror is uncertain.

The behaviour of egress mirror port should be the consistent to the output port.eg:port2 is the egress port,and port 3 is the mirror port(mirror the dst traffic of port 2).If the switch support egress mirror(egress mirror is true),then the packets of port 2 are tagged packets,then traffic of port 3 are also tagged packets.

Configuration Examples

The following examples show how to configure the port mirroring feature.

```
admin@PicOS-OVS$ovs-vsctl -- set bridge br0 mirrors=@m -- --id=@te-1/1/1 get Port te-1/1/1 -- --id=@te-1/1/2 get Port te-1/1/2 -- -
admin@PicOS-OVS$
```

The configuration above includes ports te-1/1/1, te-1/1/2 and te-1/1/3. The source ports are te-1/1/1 and te-1/1/2 (including ingress and egress), and the output port (monitor port) is te-1/1/3.

The "select-dst-port" means some packets (in switch chip) will go-out from the specified port (egress).

The "select-src-port" means some packets will enter the specified port (ingress).

> PicOS can support multiple mirrors, but some limitations exist.
>
> 1. Only has one output port, at this time the specified port can be configure multiple ways..
>
> 2. If configure different output ports, the max monitor port at most is 4.
>
> 3, Before PicOS2.10 ovs only support configure physical port as output_port, from PicOS2.10 ovs also support lag interface as output_port.

The command set 2 mirrors, m1 and m2:

```
admin@PicOS-OVS$ovs-vsctl -- set bridge br0 mirrors=@m1,@m2 -- --id=@te-1/1/11 get Port te-1/1/11 -- --id=@te-1/1/13 get Port te-1/
```

The command add 2 new mirrors, m3 and m4:

```
admin@PicOS-OVS$ovs-vsctl add bridge br0 mirrors @m3,@m4 -- --id=@te-1/1/11 get Port te-1/1/11 -- --id=@te-1/1/12 get Port te-1/1/1
```

Deleting the Mirroring

```
root@PicOS-OVS# ovs-vsctl clear Bridge br0 mirrors
```

> **limitations for tomahawk**
> For tomahawk chip,do not support mirror ingress dirction and egress direction for the same port.

OVSDB file

The PicOS switch stores the OVS (Open vSwitch) configuration in **/ovs/ovs-vswitchd.conf.db**.

```
admin@PicOS-OVS$cd /ovs
admin@PicOS-OVS$ls
bin  function.conf.db  ovs-vswitchd.conf.db  sbin   snmp
etc  lib               portGroup.conf.db     share  var
```

OVS LLDP

The **Link Layer Discovery Protocol** (**LLDP**) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on ethernet networks. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery* specified in standards document **IEEE 802.1AB**

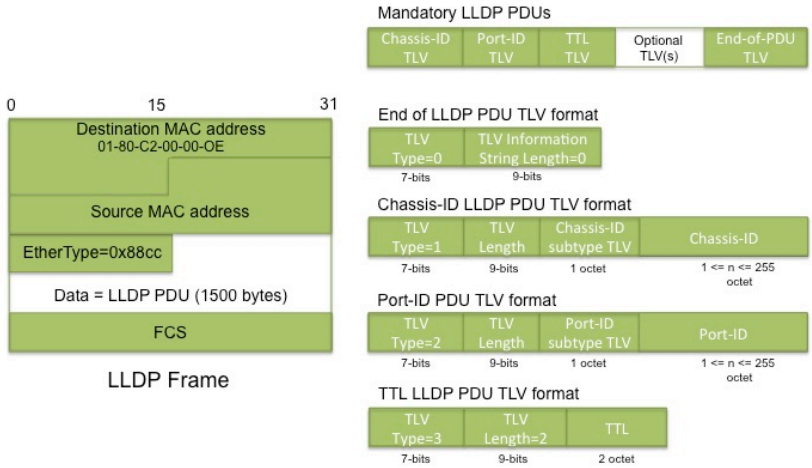


Figure1: LLDP packet format and the mandatory LLDP PDUs

The LLDP frame consists of the following:

1. a well know destination multicast address (01:80:C2:00:00:0E)
2. ether type of 0x88cc
3. LLDP PDU consisting of the following mandatory LLDP TLVs:
    a. Chassis TLV: Identifies the 802 LAN device's chassis.
    b. Port-ID TLV: Identifies the port from which the LLDPDU is transmitted.
    c. TTL TLV: Indicates how long (in seconds) the LAN device's information received in the LLDPDU is to be treated as valid information. Non-zero information indicates the device's information is to be updated in the LLDP remote system MIB. A value of 0 indicates the information associated with the LAN device is no longer valid and should be removed.
    d. End-of-LLDP TLV: Indicates the end of TLVs in the LLDPDU.

Typically, an open flow controller uses LLDP messages to discover neighbor devices, active links and hosts connected to the open flow switches. Following represents a typical flow used to relay LLDP messages from an open flow switch to the controller

dl_dst=01:80:c2:00:00:0e,dl_type=0x88cc, actions:CONTROLLER

Alternatively LLDP can be enabled in PicOS. PicOS supports the following LLDP TLVs:

1. *Port Description TLV*
2. *System Name TLV*
3. *System Description TLV*
4. *System Capabilities TLV*
5. *Management Address TLV.*802.1
6. Organizationally Specific TLV includes:
    a. *PVID TLV* (The default value is false)
    b. *MAC PHY TLV* (The default value is false)
    c. *MDI TLV* (The default value is false)
    d. Max Frame Size TLV (The default value is false)

> PicOS supports LLDP from version 2.6.

LLDP commands

Enable or disable lldp on bridge

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 lldp_enable=true
admin@PicOS-OVS$ovs-vsctl clear bridge br0 lldp_enable
```

LLDP admin status

```
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 lldp_admin_status=RxTx
```

```
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 lldp_admin_status=RxOnly
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 lldp_admin_status=TxOnly
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 lldp_admin_status=disabled
```

LLDP transmit parameters

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-msg-tx-hold=4
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-msg-tx-interval=30
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-reinit-delay=2
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tx-delay=2
```

LLDP transmit parameters on a per interface

```
ovs-vsctl set interface te-1/1/25 lldp_tx_interval=4
ovs-vsctl set interface te-1/1/25 lldp_tx_delay=2

clear commands:
ovs-vsctl clear interface te-1/1/14 lldp_tx_interval
ovs-vsctl clear interface te-1/1/14 lldp_tx_delay
```

Optional TLVs in lldpdu

Port Description TLV (The default value is true)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-port-desc=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-port-desc=false
```

System Name TLV (The default value is true)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-name=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-name=false
```

System Description TLV (The default value is true)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-desc=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-desc=false
```

System Capabilities TLV (The default value is true)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-cap=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-cap=false
```

Management Address TLV (The default value is true)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mgmt-addr=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mgmt-addr=false
```

PVID TLV (802.1 Organizationally Specific TLV) (The default value is false)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-pvid=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-pvid=false
```

MAC PHY TLV (802.3 Organizationally Specific TLV) (The default value is false)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mac-phy=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mac-phy=false
```

Power Via MDI TLV (802.3 Organizationally Specific TLV) (The default value is false)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-power-via-mdi=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-power-via-mdi=false
```

Link Aggregation TLV (802.3 Organizationally Specific TLV) (The default value is false)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-link-aggregation=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-link-aggregation=false
```

Max Frame Size TLV (802.3 Organizationally Specific TLV) (The default value is false)

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-max-frame-size=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-max-frame-size=false
```

show configuration

```
admin@PicOS-OVS$ovs-vsctl list bridge br0
admin@PicOS-OVS$ovs-vsctl list interface ge-1/1/1
```

show LLDP remote neighbors

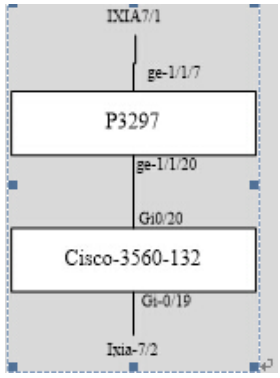
```
admin@PicOS-OVS$ovs-vsctl list lldp_neighbor
```

show LLDP using "ovs-appctl"

```
admin@PicOS-OVS$ovs-appctl lldp/show br0
admin@PicOS-OVS$ovs-appctl lldp/show br0 ge-1/1/1
```

Examples

topology



default port status test

Cisco3560 (mac 00:22:BE:96:F5:94):

```
Switch#configure terminal
Switch(config)#lldp run(default status is TXRx)
Switch(config)#monitor session 1 source interface gigabitEthernet 0/20 rx
Switch(config)#monitor session 1 destination interface gigabitEthernet 0/19
```

P3297 (mac 00:e0:ec:25:2d:5e):

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 lldp_enable=true
not  set lldp_admin_status(default value is RxTx)
admin@PicOS-OVS$ovs-vsctl list lldp_neighbor
_uuid               : dc8a0cba-aefd-4b54-b02f-e53b315fd783
local_id            : "<00:e0:ec:25:2d:5e>:<ge-1/1/20>"
mgmt_address        : {"10.10.51.132"=0}
```

```
port_description    : "GigabitEthernet0/20"
remote_id           : "<00:22:be:96:f5:80>:<Gi0/20>"
system_description  : "Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0(2)SE2, RELEASE SOF
system_name         : Switch
admin@PicOS-OVS$
```

Result:

7/1: receive the lldp from both Cisco3560 and P3297

7/2: only receiving the lldp with src mac **00:e0:ec:25:2d:5e**

note

1. LLDP only works on physical ports；
2. PicOS does not support power-via-mdi TLV;
3. 1=<lldp-tx-delay<=0.25*msg-tx-interval;

Enabling Radius in PicOS OVS Mode

Perform the following steps to enable Radius in PicOS OVS mode:

1. Enable user map

```
admin@PicOS-OVS$sudo /pica/bin/usermap_disable.sh false
```

2. Enable Radius on the PicOS switch.

```
admin@PicOS-OVS$sudo /pica/bin/radius_disable.sh false
```

3. Configure the IP address of the external Radius server on the PicOS switch. In the following example, IP address of the Radius server is 1.1.5.41 and the shared key is *abc*.

```
admin@XorPlus$cat /etc/pam_radius_auth.conf
1.1.5.41:1812 abc 1
```

4. Users on the Radius server must be super users. The following example shows the Radius record for user *test8*.

```
test8 Cleartext-Password := "pica8"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 172.16.3.33,
Framed-IP-Netmask = 255.255.255.0,
Framed-Routing = Broadcast-Listen,
Framed-Filter-Id = "std.ppp",
Framed-MTU = 1500,
Framed-Compression = Van-Jacobsen-TCP-IP,
Class = "super-user"
```

5. Login to the switch via SSH and execute Linux shell commands.

```
build@dev-18:$ ssh 10.10.51.145 -l test8
test8@10.10.51.145's password:
test8@PicOS-OVS:~$ version
Copyright (C) 2009-2014 Pica8, Inc.
==================================
Hardware Model                : P-3290
Linux System Version/Revision : 1.1/20809
Linux System Released Date    : 03/21/2015
L2/L3 Version/Revision        : 1.1/20809
L2/L3 Released Date           : 03/21/2015
OVS/OF Version/Revision       : 1.1/20809
OVS/OF Released Date          : 03/21/2015
test8@PicOS-OVS:~$ pwd
/home/test8
test8@PicOS-OVS:~$
```

6. The Radius user must use the full path to execute OVS commands, as shown below:

```
test8@PicOS-OVS$sudo /ovs/bin/ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2): dpid:5e3ee89a8f503d30
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
 1(ge-1/1/1): addr:e8:9a:8f:50:3d:30
     config:     0
     state:      LINK_DOWN
     current:    COPPER AUTO_NEG
     advertised: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     speed: 0 Mbps now, 1000 Mbps max
 LOCAL(br0): addr:e8:9a:8f:50:3d:30
     config:     0
     state:      LINK_UP
```

```
     current:    10MB-FD COPPER
     supported:  10MB-FD COPPER
     speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.4) (xid=0x5): frags=normal miss_send_len=0

test8@PicOS-OVS:~$ sudo ovs-vsctl show
395575df-5939-45af-8e4c-d99da4c442dc
    Bridge "br0"
        Port "ge-1/1/1"
            tag: 1
            Interface "ge-1/1/1"
                type: "pica8"
        Port "br0"
            Interface "br0"
                type: internal
```

7. User can also modify the path by editing the */etc/sudoers* file, so that Radius users can execute OVS commands directly. Change the value of **Defaults secure_path** from "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/ovs/bin:/ovs/sbin" to another desired value.

```
test8@PicOS-OVS:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/ovs/bin:/ovs/sbin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%xorp ALL=(ALL) NOPASSWD: NOPASSWD: ALL
%root ALL=(ALL) NOPASSWD: NOPASSWD: ALL
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
```

Inventory Database

Introduction

Pica-OVS mode switch needs to store some basic switch information and some run-time information in the inventory database, this feature is running when Pica-OVS starts.

There are five kinds of information in this module as shown below, including basic Switch Information, SFP/QSFP Information, Counter Information, Alarm Information, and Hardware Flow Information.

Switch Information

Show function control information.

```
root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
  sfp_enable: true
  sfp_query_interval: 10
  counter_enable: false
  hwflow_enable: false
  counter_query_interval: 30
  hwflow_query_interval: 30
  alarm_enable: false
  alarm_high_temp: 176
  alarm_low_temp: 32
  last_alarm_id: 0
```

Show basic switch information in the Switch Inventory table, including switch information, temperature information, port information and SFP/QSFP information.

> Before checking the switch information, the DUT must create a bridge and add ports into the bridge. Then make sfp enable-true.

```
root@PicOS-OVS$ovs-invctl enable-sfp true

root@PicOS-OVS$ovs-invctl show-switch-inventory
2ef72735-5c91-43a3-9c95-cb16dd8b2cd7
  model: "P3295"
  system_mac: "e8:9a:8f:50:3d:30"
  vendor_name: "Pica8"
  serial_number: "QTFAXI12400017"
  ge_port_number: 48
  te_port_number: 4
  qe_port_number: 0
  cpu_temperature: "100 F"
  switch_temperature: "100 F"
  system_temperature: "93 F"
  7c40378e-751f-470f-a8ad-7176a9c16b2c
    port_name: "te-1/1/50"
    vendor_name: JESS-LINK
    vendor_sn: "12344D0001"
    wavelength: "256 nm"
    temperature: "32 F"
    supply_voltage: "0.00 V"
    connector: "Copper pigtail"
    length_copper: "5 m"
    length_50m: "0 m"
    length_625m: "0 m"
    length_9m: "0 m"
    length_9m_km: "0 m"
    plugged_in: true
    rx_receive_power: "-inf dbM"
    tx_bias_current: "0.00 mA"
    tx_optical_power: "-inf dbM"
```

SFP/QSFP Information

SFP/QSFP information is stored into the database if user enables this feature. The Administrator could enable/disable this function by using command "ovs-invctl enable-sfp {true | false}".

```
root@PicOS-OVS$ovs-invctl enable-sfp true

Administrator could show these information by command "ovs-invctl show-switch-inventory" or "ovs-invctl show-sfp-qs

root@PicOS-OVS$ovs-invctl show-sfp-qsfp
84cb20bd-4ddc-4094-aaaa-b36dc59332a9
  port_name: "te-1/1/49"
  vendor_name: JESS-LINK
  vendor_sn: "12344D0001"
  wavelength: "256 nm"
  temperature: "32 F"
  supply_voltage: "0.00 V"
  connector: "Copper pigtail"
  length_copper: "5 m"
  length_50m: "0 m"
  length_625m: "0 m"
  length_9m: "0 m"
  length_9m_km: "0 m"
  plugged_in: true
  rx_receive_power: "-inf dbM"
  tx_bias_current: "0.00 mA"
  tx_optical_power: "-inf dbM"
```

Administrator could control the refresh interval by command "ovs-invctl set-sfp-interval."

```
root@PicOS-OVS$ovs-invctl set-sfp-interval 50
root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
 sfp_enable: true
 sfp_query_interval: 50
 counter_enable: false
 hwflow_enable: false
 counter_query_interval: 30
 hwflow_query_interval: 30
 alarm_enable: false
 alarm_high_temp: 176
 alarm_low_temp: 32
 last_alarm_id: 0
```

Counter Information

There are 4 types of counters: flow, group, meter, and port counter. As expected, the flow counter is the counter of each flow and the port counter is the counter of each port. The meter counter is the counter of each meter, associated with the band counter, and the group counter is the counter of each group, associated with the bucket counter.

> Note: this kind of information generates a lot of data. Turning this on will spend some CPU and memory. So if this information is not needed, please turn it off.

Administrator could enable/disable this function by command **"ovs-invctl enable-counter {true | false}"**

```
root@PicOS-OVS$ovs-invctl enable-counter true
```

Administrator could control the refresh interval by command **"ovs-invctl set-counter-interval"**.

```
root@PicOS-OVS$ovs-invctl enable-counter true
root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
 sfp_enable: true
 sfp_query_interval: 50
 counter_enable: true
 hwflow_enable: false
```

```
 counter_query_interval: 20
 hwflow_query_interval: 30
 alarm_enable: false
 alarm_high_temp: 176
 alarm_low_temp: 32
 last_alarm_id: 0
```

The Administrator could show this information by command **"ovs-invctl show-port/meter/flow/group-counter"** or **"ovs-invctl show-all-counter"**.

```
root@PicOS-OVS$ovs-invctl show-all-counter
Switch PicOS-OVS
  Bridge "br0"
    Port "Bridge br0 Local Port"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=368, rx_
    Port "Bridge br0 Port 50"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=0, rx_cr
    Port "Bridge br0 Port 49"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=0, rx_cr

root@PicOS-OVS$ovs-invctl show-port-counter
Switch : PicOS-OVS
  Bridge : br0
    Port "Bridge br0 Local Port"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=368, rx_
    Port "Bridge br0 Port 49"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=0, rx_cr
    Port "Bridge br0 Port 50"
      statistics: {collisions=0, duration_nsec=3220239464, duration_sec=1208147968, multicast=0, rx_bytes=0, rx_cr
```

Alarm Information

Alarm stores the alarm information about: PSU, FAN, OPTICS, PORT, TEMP, MANAGEMENT_PORT_STATUE. This information is stored in the Alarm table.

Administrator could enable/disable this function by command "ovs-invctl enable-alarm {true | false}".

```
root@PicOS-OVS$ovs-invctl enable-alarm true

root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
  sfp_enable: true
  sfp_query_interval: 50
  counter_enable: true
  hwflow_enable: false
  counter_query_interval: 20
  hwflow_query_interval: 30
  alarm_enable: true
  alarm_high_temp: 176
  alarm_low_temp: 32
  last_alarm_id: 9
```

The Administrator could control the temperature threshold by the command **"ovs-invctl set-high/low-temp"**. When the switch temp id is higher or lower then the temperature threshold, it will produce an alarm message.

```
root@PicOS-OVS$ovs-invctl set-low-temp 10
root@PicOS-OVS$ovs-invctl set-high-temp 133

root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
  sfp_enable: true
  sfp_query_interval: 50
  counter_enable: true
  hwflow_enable: false
  counter_query_interval: 20
  hwflow_query_interval: 30
  alarm_enable: true
  alarm_high_temp: 133
```

```
  alarm_low_temp: 10
  last_alarm_id: 9
```

The Administrator could show this information by the command **"ovs-invctl show-alarm"**

```
root@PicOS-OVS$ovs-invctl show-alarm
Alarm 1
  severity_code: cleared
  switch_name: PicOS-OVS
  entity_text: "te-1/1/50"
  text: "Optics inserted"
  time: "Tue Nov  3 13:49:28 2015"
Alarm 2
  severity_code: cleared
  switch_name: PicOS-OVS
  entity_text: "te-1/1/49"
  text: "Optics inserted"
  time: "Tue Nov  3 13:49:28 2015"
Alarm 3
  severity_code: critical
  switch_name: PicOS-OVS
  entity_text: "power 1"
  text: "power removed"
  time: "Tue Nov  3 13:49:39 2015"
Alarm 4
  severity_code: critical
  switch_name: PicOS-OVS
  entity_text: "PSU 1"
  text: "PSU removed"
  time: "Tue Nov  3 13:49:39 2015"
```

Hardware Flow Information

Note: This kind of information is very large, turning this feature on will spend some CPU and memory. So if this information is not needed, please turn it off. For saving memory, we support max 20,000 hardware flows written into the database. If the count of hardware flows is exceeded, they are discarded.

Administrator could enable/disable this function by the command **"ovs-invctl enable-hwflow {true | false}"**.

```
root@PicOS-OVS$ovs-invctl enable-hwflow true

root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
  sfp_enable: true
  sfp_query_interval: 50
  counter_enable: true
  hwflow_enable: true
  counter_query_interval: 20
  hwflow_query_interval: 30
  alarm_enable: true
  alarm_high_temp: 133
  alarm_low_temp: 10
  last_alarm_id: 9
```

The Administrator could control the refresh interval by command **"ovs-invctl set-hwflow-interval INTEGER"**.

```
root@PicOS-OVS$ovs-invctl enable-hwflow true

root@PicOS-OVS$ovs-invctl set-hwflow-interval 50
root@PicOS-OVS$ovs-invctl show
23aa0580-9578-471a-abae-a9c84b73affd
  sfp_enable: true
  sfp_query_interval: 50
  counter_enable: true
```

```
  hwflow_enable: true
  counter_query_interval: 20
  hwflow_query_interval: 50
  alarm_enable: true
  alarm_high_temp: 133
  alarm_low_temp: 10
  last_alarm_id: 9
```

The Administrator could get hardware flow information by the command **"ovs-invctl list Hardware_Flow"**

Others Hardware_Flow commands are available by using the command **"root@PicOS-OVS$ovs-invctl --help"**

```
root@PicOS-OVS$ovs-invctl list Hardware_Flow
_uuid               : e6e61c9d-df38-43c6-abc0-2b0654af9713
hwflow              : "[\"#0 normal_d permanent priority=0,recirc_id=0, actions:drop\", \"#1 normal permanent recir
update_time         : "Tue Nov  3 15:11:19 2015"
```

Show Power/Fan Information

```
root@PicOS-OVS$ovs-invctl list power-status
_uuid               : 19af5a8c-9adc-4d92-8615-0e4a50aadabd
good_12v            : "false"
led                 : ""
number              : 1
power_alert         : ""
present             : "false"

_uuid               : 95b3fa12-8f6e-4709-bf0a-363a9fda0c2f
good_12v            : "true"
led                 : ""
number              : 2
power_alert         : ""
present             : "true"

root@PicOS-OVS$ovs-invctl list fan_status
_uuid : 43d903ec-7894-4df7-833b-5d5a1004b388
direction : "fan direction from front to back"
fault : "false"
input : " 11400 rpm"
number : 3
pwm : " 50 %"
```

Broadcom Chip Limitation in OVS

ARP Flow in Combinated Mode Table

Due to VCAP limitation, ARP flow entry will generate an error once combinated-mode is enabled.

When combinated mode is enabled, VCAP needs to match the same fields as ICAP. ARP flows use UDF in ICAP, but not all HW platforms support UDF in VCAP.

Example:

```
ovs-vsctl set-combinated-mode true
admin@PicOS-OVS$ovs-ofctl dump-flows br2
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=70.192s, table=0, n_packets=n/a, n_bytes=0, priority=500,arp actions=output:2
 cookie=0x0, duration=6.928s, table=0, n_packets=n/a, n_bytes=0, priority=200,in_port=7 actions=push_vlan:0x8100,set_field:2001->vl
```

Actual result:

sent packets match both flows to ge-1/1/7,ge-1/1/2 will receive packets that with "push_vlan:0x8100,set_field:2001->vlan_vid",ge-1/1/8 will not receive any packets.

Overlap flow

Because some limitation of ASIC, some flow installed hardware can not work as expected. User should refer to this chapter before user starts to trouble-shoot the issues.

udp/ip, tcp/ip

When user adds flows with the same priority, and one flow's match fields includes another flow's match fields, the action of flow is at random. For example:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=10000,ip,in_port=14,dl_vlan=2,actions=push_vlan:0x8100,set_field:2503-\>vlan_vid,ou
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#40 permanent priority=10000,ip,in_port=14,dl_vlan=2, actions:push_vlan(vid=2503),mod_vlan_pcp(pcp=0),15
Total 1 flows in TCAM.
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=10000,udp,in_port=14,dl_vlan=2,tp_dst=2123,actions=push_vlan:0x8100,set_field:2500-
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#41 permanent priority=10000,udp,in_port=14,dl_vlan=2,tp_dst=2123, actions:push_vlan(vid=2503),mod_vlan_pcp(pcp=0),15
#40 permanent priority=10000,ip,in_port=14,dl_vlan=2, actions:push_vlan(vid=2503),mod_vlan_pcp(pcp=0),15
Total 2 flows in TCAM.
```

If user doesn't want this result, user should modify the two flows' priorities.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=12000,udp,in_port=14,dl_vlan=2,tp_dst=2123,actions=push_vlan:0x8100,set_field:2500-
ovs-ofctl add-flow br0 priority=10000,ip,in_port=14,dl_vlan=2,actions=push_vlan:0x8100,set_field:2503-\>vlan_vid,output:15
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#42 permanent priority=12000,udp,in_port=14,dl_vlan=2,tp_dst=2123, actions:push_vlan(vid=2500),mod_vlan_pcp(pcp=0),15
#40 permanent priority=10000,ip,in_port=14,dl_vlan=2, actions:push_vlan(vid=2503),mod_vlan_pcp(pcp=0),15
Total 2 flows in TCAM.
```

Priority of Arp flow

Generally, the priority of an arp group is higher than a mac group. If one flow matches arp group and mac group at the same time, even if the priority of the arp is lower than the mac, packets will be forwarded according to arp group.

Example 1

Basic configuration:

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1-- set interface ge-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1-- set interface ge-1/1/4 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/5 vlan_mode=trunk tag=1-- set interface ge-1/1/5 type=pica8
```

Add flow:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=ff:ff:ff:ff:ff:ff,actions=5
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0806,arp_op=1,actions=4
```

Check table:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#3720 normal permanent recirc_id=0,arp,in_port=1,arp_op=1, actions:4
#3719 normal permanent recirc_id=0,in_port=1,dl_dst=ff:ff:ff:ff:ff:ff, actions:5
#3718 normal permanent priority=0,recirc_id=0, actions:drop
Total 3 flows in HW.
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=28.919s, table=0, n_packets=n/a, n_bytes=0, in_port=1,dl_dst=ff:ff:ff:ff:ff:ff actions=output
cookie=0x0, duration=15.884s, table=0, n_packets=n/a, n_bytes=0, arp,in_port=1,arp_op=1 actions=output:4
admin@PicOS-OVS$
```

Send arp request packets and then check table:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=62.999s, table=0, n_packets=n/a, n_bytes=0, in_port=1,dl_dst=ff:ff:ff:ff:ff:ff actions=output
cookie=0x0, duration=49.964s, table=0, n_packets=n/a, n_bytes=2560000, arp,in_port=1,arp_op=1 actions=output:4
```

From example above, if packets match files of above flows, packets will be forwarded according to arp.

Example 2

Add flow:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,priority=333,dl_dst=ff:ff:ff:ff:ff:ff,actions=5
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,priority=222,dl_type=0x0806,arp_op=1,actions=4
```

Send arp request packets and check table:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=19.544s, table=0, n_packets=n/a, n_bytes=0, priority=333,in_port=1,dl_dst=ff:ff:ff:ff:ff:ff a
cookie=0x0, duration=8.422s, table=0, n_packets=n/a, n_bytes=19846144, priority=222,arp,in_port=1,arp_op=1 actions=
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=20.931s, table=0, n_packets=n/a, n_bytes=0, priority=333,in_port=1,dl_dst=ff:ff:ff:ff:ff:ff a
cookie=0x0, duration=9.809s, table=0, n_packets=n/a, n_bytes=26813440, priority=222,arp,in_port=1,arp_op=1 actions=
admin@PicOS-OVS$
```

Even if arp group priority is lower than mac group, packets still are forwarded according to arp group.

Vlan Isolation

Vlan Isolation

At the moment, the vlan isolation only works on the egress of a port, not on the ingress direction.

Limitations on trident3

Limitation1:double 'pop_vlan' actions in flow entry on trident3 chip.

delete inner and outer tags in vcap, icap does not match any vlan tag.So may mismatch other packets in icap at this time.

Example:

Add a flow with double ‘pop_vlan’:

```
ovs-ofctl add-flow br0 in_port=1,dl_vlan=200,actions=pop_vlan,pop_vlan,output:2
```

send packets

send packets with outer vlan is 200,inner vlan is 100,then this kinds of packets can be transmitted correctly after pop these two vlans.Send others packets which outer vlan is not 200 or untag packets to port 1,then all the packets may be transmitted by port 2.But theoretically,the packets should not match the above flow.

Limitation2:TD3(s5248,as7326_56x,7726) and Tomahawk don't support egress-meter.

Limitation3:tcam usage

TD3 platforms icap entries max limitation is 3k, even if enable match-mode, the value is still 3k.

Limitation4:Trident3 does not support ingress-rate-limit.

Limitations5:Pop mpls

1) pop one mpls label,match fields exist only one mpls_label.

send packets with only one mpls label,then in SDK match mpls label finally.

2) pop one mpls label,match fields exist two mpls_labels.

send packets with two mpls labels(label1,label2),then in SDK match mpls label1 finally.

3) pop two mpls labels,match fields exist two mpls_labels.then in SDK match mpls label2 finally.

OVS CLI Enhancements

PicOS OVS cli has some enhancements from version 2.7.1.

List ovs running configuration

From PicOS2.7.1 OVS add a new command to display the current configuration by traversing the ovsdb tables. The command is:

ovs-vsctl show-running-config

```
admin@PicOS-OVS$ovs-vsctl show-running-config
Open_vSwitch c645ee8a-34d5-4c64-a3dc-0c1a20f3c26e
  Bridge "br0"
    datapath_id: "1c48cc37ab254bc1"
    datapath_type: "pica8"
    Port "ge-1/1/19"
      Interface "ge-1/1/19"
        type: "pica8"
      tag: 1
      vlan_mode: trunk
    Port "br0"
      Interface "br0"
        mtu: 1500
        type: internal
  Pica8 ecafe6f4-97ac-407b-b4df-c871b5cd9561
    hardware_type: "as4610_54t"
admin@PicOS-OVS$
```

Show ovs-vsctl commands

From PicOS3.2.0, OVS add one command to show the configurations in ovsdb through ovs-vsctl command.

ovs-vsctl display-settings

```
admin@PICOS-OVS:~$ ovs-vsctl display-settings
ovs-vsctl add-br br0
ovs-vsctl add-port br0 ge-1/1/1
ovs-vsctl set port ge-1/1/1  vlan_mode=trunk  tag=1
ovs-vsctl set interface ge-1/1/1  options=link_speed=100M
ovs-vsctl add-port br0 ge-1/1/2
ovs-vsctl set port ge-1/1/2  vlan_mode=trunk  tag=1
ovs-vsctl set interface ge-1/1/2  options=mtu=1500
ovs-vsctl set-group-ranges ecmp-select-groups=1-100
ovs-vsctl set-match-mode ip=1-1000,ipv6_full=1001-2000
```

List System Resources Usage

From PicOS2.7.1 OVS add two commands to display current system resources usage and interfaces.

When we show system resources usage, the current mode is cared, such as match-mode, udf-mode, L2-mode, L3-mode, combinate-mode and egress-mode.

The commands are:

ovs-appctl pica/show tables

ovs-appctl pica/show interfaces

```
admin@PicOS-OVS$ovs-appctl pica/show tables
Pica Tables Statistics:
    Pica Tables              Max Limitation          Current Used
    ------------------------------------------------------------------------
    ICAP Table                 2046                    9
    ECAP Table                 (null)                  (null)
    VCAP Table                 1024                    0
    L2 System Table            (null)                  (null)
    L2 FDB Table               (null)                  (null)
    L3 Host Table              (null)                  (null)
    L3 Route Table             (null)                  (null)
```

```
    UDF Table                 (null)                 (null)
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/show interfaces
Valid Interfaces On Switch P3290:
Physical interfaces:
ge-1/1/1(1) ge-1/1/2(2) ge-1/1/3(3) ge-1/1/4(4)
ge-1/1/5(5) ge-1/1/6(6) ge-1/1/7(7) ge-1/1/8(8)
ge-1/1/9(9) ge-1/1/10(10) ge-1/1/11(11) ge-1/1/12(12)
ge-1/1/13(13) ge-1/1/14(14) ge-1/1/15(15) ge-1/1/16(16)
ge-1/1/17(17) ge-1/1/18(18) ge-1/1/19(19) ge-1/1/20(20)
ge-1/1/21(21) ge-1/1/22(22) ge-1/1/23(23) ge-1/1/24(24)
ge-1/1/25(25) ge-1/1/26(26) ge-1/1/27(27) ge-1/1/28(28)
ge-1/1/29(29) ge-1/1/30(30) ge-1/1/31(31) ge-1/1/32(32)
ge-1/1/33(33) ge-1/1/34(34) ge-1/1/35(35) ge-1/1/36(36)
ge-1/1/37(37) ge-1/1/38(38) ge-1/1/39(39) ge-1/1/40(40)
ge-1/1/41(41) ge-1/1/42(42) ge-1/1/43(43) ge-1/1/44(44)
ge-1/1/45(45) ge-1/1/46(46) ge-1/1/47(47) ge-1/1/48(48)
te-1/1/49(49) te-1/1/50(50) te-1/1/51(51) te-1/1/52(52)
LAG interfaces: ae1(1025) - ae1023(2047)
Bond interfaces: bond1(2049) - bond1023(3071)
GRE interfaces: gre1(3073) - gre1023(4095)
VXLAN interfaces: vxlan1(4097) - vxlan1023(5119)
L2GRE interfaces: l2gre1(5121) - l2gre1023(6143)
admin@PicOS-OVS$
```

Associate sw-flow with hw-flow

From PicOS2.7.1, when a new flow entry is added, a unique 64bit flow-id is assigned to it. The flow-id can be used by ovs-ofctl and ovs-appctl to filter the flow entries and associate sw-flow with hw-flow.

The commands are:

ovs-ofctl dump-flows br0 [flow_id=n]

ovs-appctl pica/dump-flows [flow_id=n]

Example 1:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 priority=200,in_port=1,actions=2
root@PicOS-OVS$ovs-ofctl add-flow br0 priority=124,in_port=1,ip,nw_src=10.10.10.10,actions=4
root@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=36.591s, flow_id=1, table=0, n_packets=n/a, n_bytes=0, priority=200,in_port=1 actions=output
 cookie=0x0, duration=6.393s, flow_id=2, table=0, n_packets=n/a, n_bytes=0, priority=124,ip,in_port=1,nw_src=10.10
root@PicOS-OVS$ovs-appctl pica/dump-flows
#4 normal permanent flow_id=1, priority=124,recirc_id=0,ip,in_port=1,nw_src=10.10.10.10, actions:2
#3 normal permanent flow_id=1, priority=200,recirc_id=0,in_port=1, actions:2
#0 normal_d permanent priority=0,recirc_id=0, actions:drop
Total 3 flows in HW.
```

From the above example, if two flow entries in table 0 don't have the exact same match and priority, but the match of sw-flow which has higher priority can cover another sw-flow's match, then two hw-flows with the same flow-id of sw-flow which has the higher priority will be installed.

Example 2:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 priority=200,in_port=1,actions=goto_table:1
root@PicOS-OVS$ovs-ofctl add-flow br0 table=1,priority=101,in_port=1,ip,nw_src=10.10.10.11,actions=2
root@PicOS-OVS$ovs-ofctl add-flow br0 table=1,priority=102,ip,nw_src=10.10.10.12,actions=goto_table:2
root@PicOS-OVS$ovs-ofctl add-flow br0 table=2,priority=123,dl_dst=00:11:22:33:44:55,actions=3
root@PicOS-OVS$
root@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=184.078s, flow_id=1, table=0, n_packets=n/a, n_bytes=0, priority=200,in_port=1 actions=goto_t
 cookie=0x0, duration=49.800s, flow_id=2, table=1, n_packets=n/a, n_bytes=0, priority=102,ip,nw_src=10.10.10.12 act
 cookie=0x0, duration=107.575s, flow_id=3, table=1, n_packets=n/a, n_bytes=0, priority=101,ip,in_port=1,nw_src=10.1
 cookie=0x0, duration=7.991s, flow_id=4, table=2, n_packets=n/a, n_bytes=0, priority=123,dl_dst=00:11:22:33:44:55 a
root@PicOS-OVS$ovs-appctl pica/dump-flows
#6 normal permanent flow_id=1, priority=201,recirc_id=0,ip,in_port=1,dl_dst=00:11:22:33:44:55,nw_src=10.10.10.12, a
#5 normal permanent flow_id=1, priority=200,recirc_id=0,ip,in_port=1,nw_src=10.10.10.11, actions:2
```

```
#0 normal_d permanent priority=0,recirc_id=0, actions:drop
Total 3 flows in HW.
```

If a flow entry in table 0 has goto action, then the flow-id will be applied to all hw-flows generated by it. Only the flow-id's of sw-flows in first table are cared now.

Display dpid in both hex and decimal

From PicOS2.7.1, when the status of bridge is shown, we add decimal numbers for dpid to display.

```
admin@PicOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2):
dpid:0x1c48cc37ab254bc1(2038103370851765185)
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
 13(ge-1/1/13): addr:cc:37:ab:25:4b:c1
     config:     0
     state:      LINK_UP
     current:    100MB-FD COPPER AUTO_NEG
     advertised: 10MB-FD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-FD 100MB-FD 1GB-FD COPPER AUTO_NEG
     peer:       10MB-HD 10MB-FD 100MB-HD 100MB-FD COPPER
     speed: 100 Mbps now, 1000 Mbps max
LOCAL(br0): addr:cc:37:ab:25:4b:c1
     config:     0
     state:      LINK_UP
     current:    10MB-FD COPPER
     supported:  10MB-FD COPPER
     speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.4) (xid=0x5): frags=normal miss_send_len=0
```

List Interface Details

From PicOS2.7.1, a command is added to display the details of a specific interface or all interfaces in the bridge. A corresponding openflow multipart message should be added by using multipart experimenter type, the controller can then get these statistics as well.

The command is:

ovs-ofctl dump-interfaces <bridge> [interface]

Example:

Add the following flow:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=13,actions=15
```

No packets:

```
admin@PicOS-OVS$ovs-ofctl  dump-interfaces br0 ge-1/1/15
PXST_INTERFACE_STATS reply (OF1.4) (xid=0x4): 1 interfaces
  ge-1/1/15(port 15):
     Traffic statistics:
        Input Packets.............................0
        Output Packets............................0
        Input Octets..............................0
        Output Octets.............................0
```

Port 13 send unicast packets to match the flow and check:

```
admin@PicOS-OVS$ovs-ofctl  dump-interfaces br0 ge-1/1/13
PXST_INTERFACE_STATS reply (OF1.4) (xid=0x4): 1 interfaces
  ge-1/1/13(port 13):
     Traffic statistics:
        Input Packets.............................3013397
        Output Packets............................0
        Input Octets..............................771429632
        Output Octets.............................0
     Transmit:
        Unicast packets...........................0
```

```
   Multicast packets.....................0
   Broadcast packets.....................0
   Packets 64 Octets.....................0
   Packets 65-127 Octets.................0
   Packets 128-255 Octets................0
   Packets 256-511 Octets................0
   Packets 512-1023 Octets...............0
   Packets 1024-1518 Octets..............0
   Oversize Packets......................0
   Total Packets Without Errors..........0
   Discarded Packets.....................0
   Total Packets With Errors.............0
   Single Collision Frames...............0
   Multiple Collision Frames.............0
   Deferred Frames.......................0
   Late Collisions.......................0
   Excessive Collisions..................0
   Pause Frames..........................0
Receive:
   Unicast packets.......................3013393
   Multicast packets.....................0
   Broadcast packets.....................0
   Packets 64 Octets.....................0
   Packets 65-127 Octets.................0
   Packets 128-255 Octets................0
   Packets 256-511 Octets................3013396
   Packets 512-1023 Octets...............0
   Packets 1024-1518 Octets..............0
   Oversize Packets......................0
   Total Packets Without Errors..........3013397
   Discarded Packets.....................0
   Total Packets With Errors.............0
   Alignment Errors......................0
   FCS Errors............................0
   Collisions............................0
   Pause Frames..........................0
```

Configuring Meter

Summary

If we don't limit the user ability to send data, then a large amount of traffic from different users could continuously make the network congested. In order to allocate the network resources to each user fairly and efficiently, the traffic should be limited. For instance, for the flow of a stream at each time interval, we only assign it a portion of the network resources to prevent network congestion caused by excessive burst.

In the ovs mode, user can configure meter to achieve interface and set the speed-limit including ingress and egress.The meter uses the token bucket to evaluate the specifications of the traffic, then makes a policy for the traffic, such as through, remark or drop.

Now we support 1R2C and 2R3C for the token bucket in the ingress meter and egress meter.

Configuration

In different hardware models, the maximum count of meters that PicOS OVS supports is different. User can use the command to check the maximum count.

And from version 2.9.2,meter capability also support pps.

```
admin@PicOS-OVS$ovs-ofctl meter-features br0
OFPST_METER_FEATURES reply (OF1.4) (xid=0x2):
max_meter:2048 max_bands:1 max_color:3
band_types: drop dscp_remark
capabilities: kbps pps burst stats
```

Ingress Meter

1R2C: Add a meter, the type=drop.

Without burst size. Limit the rate as 300000 kbps.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=300000
```

With burst size. Limit the rate as 300000 kbps and burst 30000 kbit

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=drop,rate=300000,burst_size=30000
```

1R2C: Add a meter, the type=dscp_remark.

Without burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,band=type=dscp_remark,rate=300000,prec_level=14
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=3,pps,band=type=dscp_remark,rate=300000,prec_level=14
```

With burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=dscp_remark,rate=300000,prec_level=14,burst_si
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=3,pps,burst,band=type=dscp_remark,rate=300000,prec_level=14,burst_size
```

Check the meter configuration

```
admin@PicOS-OVS$ovs-ofctl dump-meters br0
OFPST_METER_CONFIG reply (OF1.4) (xid=0x2):
meter=2 kbps burst bands=
type=dscp_remark rate=300000 burst_size=30000 prec_level=14
meter=3 pps burst bands=
type=dscp_remark rate=300000 burst_size=30000 prec_level=14
admin@PicOS-OVS$
```

Modify one meter

```
root@LNOS-OVS$ovs-ofctl mod-meter br0 meter=2,kbps,burst,band=type=dscp_remark,
```

```
rate=400000,prec_level=1,burst_size=10000
root@LNOS-OVS$
root@LNOS-OVS$ovs-ofctl dump-meters br0
OFPST_METER_CONFIG reply (OF1.4) (xid=0x2):
meter=2 kbps burst bands=
type=dscp_remark rate=400000 burst_size=10000 prec_level=1
root@LNOS-OVS$
```

Dump meter stats

```
admin@PicOS-OVS$ovs-ofctl meter-stats br0
```

Delete one meter or all meters

```
root@LNOS-OVS$ovs-ofctl del-meter br0 meter=2
root@LNOS-OVS$
root@LNOS-OVS$ovs-ofctl del-meters br0
root@LNOS-OVS$
```

Notice: If one meter applies to multiple flow entries, all the flow entries will share the meter rate.

Example:

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=300000
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:11,dl_type=0x0800,a
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=12,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:22,dl_type=0x0800,a
```

1.Each in_port are sent 200M flow to one output port.

The result: the port te-1/1/13,receive 300M flow,all of flow are green,the 100M red flow are dropped.

2R3C:

Without burst size.

The first bucket limit the rate as 300000 kbps,if the rate more than it and less then 600000 kbps,the packets dscp value wiil be remarked 14.

The second bucket limit the rate as 600000 kbps, if the rate more than it,then beyond the part will be dropped.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,bands=type=dscp_remark,rate=300000,prec_level=14,type=drop,rate
```

With burst size. Limit the rate as 300000 kbps , 600000 kbps and burst as 10000 kbit, 20000 kbit.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,bands=type=dscp_remark,rate=300000,burst_size=10000,prec_
```

Example:

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,bands=type=dscp_remark,rate=300000,prec_level=14,type=drop,rate
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:11,dl_type=0x0800,a
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=12,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:22,dl_type=0x0800,a
```

1. Each in_port are sent 200M flow to one output port.

The result: the port te-1/1/13 is receive 400M flow,including 300M green flow,and 100M yellow,no red flow.

2. Each in_port are sent 300M flow to one output port.

The result: the port te-1/1/13 is receive 500M flow,including 300M green flow, 200M yellow flow, and 100M red flow are dropped.

Egress Meter

Egress meter need redistribute meter id, and it can't be used by ingress meter. After configuring,need restart the ovs service.

```
root@LNOS-OVS$ovs-vsctl set-meter-ranges egress-meter=3-4
  Please reboot for the change to take effect!
root@LNOS-OVS$systemctl restart picos
```

Check egress meter configuration

```
root@LNOS-OVS$ovs-vsctl show-meter-ranges
meter_ranges:
  egress-meter=3-4
root@LNOS-OVS$
```

The egress meter configuration is the same as ingress meter.And egress meter is also support 1R2C and 2R3C.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=3,kbps,bands=type=dscp_remark,rate=300000,prec_level=14,type=drop,rate

root@PicOS-OVS$ovs-ofctl add-meter br0 meter=4,pps,bands=type=dscp_remark,rate=300000,prec_level=14,type=drop,rate=
```

Then put a flow need applying egress meter.

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,ip,nw_src=1.1.1.2,actions=egress_meter:3,output:38
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=14,ip,nw_src=1.1.1.2,actions=egress_meter:4,output:38
```

Notice:

1.The meter configure at most two bands now in a meter flow. If only one band is set, 1R2C is effective; otherwise, 2R3C is used, and the rate configured in band1 should be smaller than rate in band2.

2.If the type of band1 is drop, the type of band2 is invalid.

3.ingress meter use color-blind mode which means the bucket don't care the color of incoming packets.

4.egress meter use color-aware mode which means the bucket can aware the color of incoming packets.

5.From version 3.4,the default burst_size value is the same with the rate user set.As following ,the burst_size is 30000kb. If the unit is pps,then the burst' unit is packets as well.The minimum value of burst is 1,when rate unit is pps,and the value is 13kb when the rate unit is kbps.

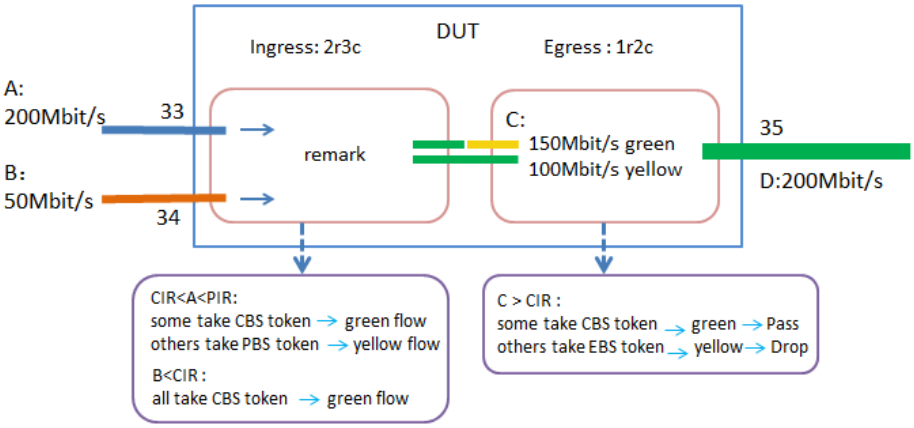
```
ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=drop,rate=30000
```

Application :

```
root@LNOS-OVS$ovs-vsctl set-meter-ranges egress-meter=3-4
  Please reboot for the change to take effect!
root@LNOS-OVS$systemctl restart picos

Ingress meter:
root@LNOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,bands=type=dscp_remark,rate=
100000,prec_level=1,type=drop,rate=300000
root@LNOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,bands=type=dscp_remark,rate=
100000,prec_level=14,type=drop,rate=300000

Egress meter:
ovs-ofctl
add-meter br0 meter=3,kbps,bands=type=drop,rate=200000

Add flow:
root@LNOS-OVS$ovs-ofctl add-flow br0 in_port=33,ip,dl_src=22:11:11:11:11:11,act
ions=meter:1,egress_meter:3,output:35
root@LNOS-OVS$ovs-ofctl add-flow br0 in_port=34,ip,dl_src=22:11:11:11:11:12,act
ions=meter:2,egress_meter:3,output:35
root@LNOS-OVS$
root@LNOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#2 normal permanent flow_id=6 ip,in_port=33,dl_src=22:11:11:11:11:11, actions:meter(id=1,band(dscp_remark=1),band(
#3 normal permanent flow_id=7 ip,in_port=34,dl_src=22:11:11:11:11:12, actions:meter(id=2,band(dscp_remark=14),band
Total 3 flows in HW.
root@LNOS-OVS$
```

Process：

sent 200M flow to port 33,50M flow to 34.



Result: the port te-1/1/35 receive 200M flow，including 150M green flow and 50M yellow flow.

Other Result:

1. Each in_port are sent 90M flow to one output port.

The result: the port te-1/1/35 receive 180M flow,all of flow are green.

2. sent 150M flow to port 33,40M flow to 34.

The result: the port te-1/1/35 receive 190M flow，including 50M yellow flow and 140M green flow.

3. Each in_port are sent 150M flow to one output port.

The result: the port te-1/1/35 receive 200M flow，including 200M green flow.

4. sent 250M flow to port 33,70M flow to 34.

The result: the port te-1/1/35 receive 200M flow，including 170M green flow and 30M yellow flow.

5. sent 350M flow to port 33,150M flow to 34.

The result: the port te-1/1/35 receive 200M flow，including 200M green flow.

6. sent 350M flow to port 33,350M flow to 34.

The result: the port te-1/1/35 receive 200M flow，including 200M green flow.

NOTICE:

1.

Simply put, the setting of the Meter parameter depends on the speed-limit of the actual traffic.
In principle, the token bucket capacity needs to be greater than or equal to the length of the largest packet and the normal burst of traffic in the network.

For the PICA8 switches, we have a summary of empirical formulas:
1.rate ≤ 100Mbit/s, token bucket capacity (kbits) = rate (Mbit/s) * 1000 (s)
2.rate > 100Mbit/s, token bucket capacity (kbits) = 100000 (kbit/s) * (s)

2.

Now, Ingress meter are supportted all platform, but egress meter just part of platform are supportted,as shown below:

NIAGARA2632XL // NIAGARA2948_6XL // S4048
PRONTO5101 // PRONTO5401 // AS6712_32X
AS5712_54X // AS6701_32X // ARCTICA4806XP
AS5812_54T

Configuration saving

Pica8 support saving configuration of meters,groups or flows which need to configure again previously after restart the switch system from version 2.8.1.

There are two scripts on /ovs/bin, ovs-pica-save and ovs-pica-load. When you have configured meters,groups or flows, please run ovs-pica-save before restart switch system. And run ovs-pica-load after restart.

Path of ovs-pica-save and ovs-pica-load: /ovs/bin

1.Configure meters.

```
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,band=type=dscp_remark,rate=300000,prec_level=14
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=300000
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=3,kbps,burst,band=type=dscp_remark,rate=300000,prec_level=14,burst_s
```

2.Configure groups.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:3
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=set_field:66:66:66:00:00:00-\>dl_src,set_f
```

3.Add flows.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,ip,dl_dst=22:22:22:22:22:22,actions=meter:1,group:1
admin@PicOS-OVS$ovs-ofctl add-flow br0 arp,arp_tpa=192.168.100.100,actions=2
```

4.Run ovs-pica-save.

```
admin@PicOS-OVS$ovs-pica-save
Meter configurations are saved to  : /ovs/config/meters
Group configurations are saved to  : /ovs/config/groups
Flow configurations are saved to  : /ovs/config/flows


Saved successfully!
admin@PicOS-OVS$
```

5.Restart the switch.

```
admin@XorPlus$sudo systemctl restart picos
```

6.Load configuration.

```
admin@PicOS-OVS$ovs-pica-load

Your configuration has been loaded successfully!
admin@PicOS-OVS$
```

If load failed,user should check files which has been saved in /ovs/config and then modify it.

7.Check after loading configuration.

```
admin@PicOS-OVS$ovs-ofctl dump-meters br0
OFPST_METER_CONFIG reply (OF1.4) (xid=0x2):
meter=1 kbps bands=
type=drop rate=300000

meter=2 kbps bands=
type=dscp_remark rate=300000 prec_level=14

meter=3 kbps burst bands=
type=dscp_remark rate=300000 burst_size=30000 prec_level=14
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-groups br0
OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
 group_id=1,type=indirect,bucket=actions=output:3
 group_id=2,type=indirect,bucket=actions=set_field:66:66:66:00:00:00->eth_src,set_field:66:66:66:11:11:11->eth_dst
```

```
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=6, cookie=0x0, duration=16.841s, table=0, n_packets=n/a, n_bytes=0, arp,arp_tpa=192.168.100.100 actions=ou
 flow_id=7, cookie=0x0, duration=16.840s, table=0, n_packets=n/a, n_bytes=0, ip,in_port=1,dl_dst=22:22:22:22:22:22
admin@PicOS-OVS$
```

Note:

1)Related configuration in br0 will save to :

Meters: /ovs/config/meters/br0

Groups: /ovs/config/groups/br0

Flows: /ovs/config/flows/br0

User can modify above files to add or delete configuration and then load new configuration.

2)If there is error information when load configuration, user can modify above files too.

3)Load meters firstly and then groups and flows lastly.

Configuring Buffer management

Introduction

When network congestion, the port cannot send data immediately to prevent loss of data, the device will send the data is temporarily stored in the data in the buffer.

1. Accounting resources

The chip stores packets in fixed-sized cells, all cells are 208 bytes and all packets user at least one cell.The first cell used by a packet contains 144 bytes of packet data and 64 bytes of buffering related data.

All cells used by a packet after the first cell contain 208 bytes of packet data.

2. Memory Spaces ：

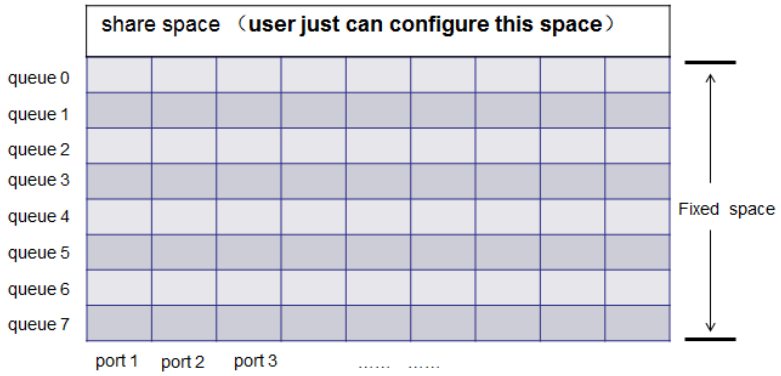
The cell data buffer is divided into fixed and shared spaces.

- Fixed space

Fixed space in accordance with the port queue division, reserved in advance, other ports cannot take up the space, when the port congestion occurs, it will occupy fixed space first, shared space will be used when the fixed space is no longer available. The fixed space is allocated using a static threshold. Fixed space allocation will not be too big, otherwise it will cause waste of resources.

- Shared space

The shared space used by all ports and priority groups when the fixed space is run out. When the shared space is used up, the packet is discarded. If a queue don't have to store packet,the others queue will take up this queue resource.For a queue,all of ports transmit packets will first come first served,if run out of the resource,the came packets will be dropped.The shared space can use dynamic or static threshold configuration at the logical level of the queue.



Command configuration

For the unicast queue and multicast queue，we have different configuration to deal with share space：

1.multicast queue：

static mode: Need configure.

- The static threshold value configured for the multicast queue in shared space.This avoids the case of the port affects the forwarding of other ports in flow control mode, but the disadvantage is that the utilization of shared resources is low.

dynamic mode : This is the default configuration.

disable queue 0 dynamic-shared

```
root@PicOS-OVS$ovs-vsctl set-egress-mc-queue-dynamic 0 false
```

2.unicast queue：

dynamic mode ：

- dynamic threshold is the default mode for the unicast queue，and it can't configure static threshold.

3.dynamic threshold ratio configuration

The dynamic mode both of multicast and unicast queue can configure the dynamic threshold ratio .

Configure queue 0 dynamic threshold ratio 50%

```
root@PicOS-OVS$ovs-vsctl set-egress-shared-queue-ratio 0 50
```

Check the configuration result

```
admin@PicOS-OVS$ovs-vsctl show-egress-shared-queue-ratio
Egress shared queue state:
    queue    uc enable   mc enable   shared ratio (uc)  shared ratio (mc)
    ------------------------------------------------------------------------
      0         true        true          33%                33%
      1         true        true          33%                33%
      2         true        true          33%                33%
      3         true        true          33%                33%
      4         true        true          33%                33%
      5         true        true          33%                33%
      6         true        true          33%                33%
      7         true        true          33%                33%
```

Clear the ratio configuration . Clear dynamic mode configuration

```
root@PicOS-OVS$ovs-vsctl list pica8
_uuid               : fef8cb42-7f42-4a1b-b089-95bf49fd7811
combinate_actions_enable: false
cos_map_enable      : false
disable_extend_group: false
ecmp_symmetric_hash : false
............
............

root@PicOS-OVS$ovs-vsctl clear pica8 fef8cb42-7f42-4a1b-b089-95bf49fd7811 egress-mc-queue-dynamic

root@PicOS-OVS$ovs-vsctl clear pica8 742a4dda-db77-474f-b702-1012141ecd5a egress_shared_queue_ratio
```

For the maximum shared-area ratio for a queue, the percentage values 0 to 100 are divided into 10 rages.The table below shows the effective values that correspond to the configured values of ratio-value.

Value of *ratio-value*	Effective value
0 to 1	1
2 to 3	3
4 to 7	6
8 to 16	11
17 to 29	20
30 to 42	33
43 to 60	50
61 to 76	67
77 to 86	80
87 to 100	89

notice
Now,all of Trident and Trident+ platforms just support eight （1-67）effective ratio value for multicast egress queue.Platform 7312,ratio of 33~100 take the same effect.

Application notice



As show above: send packets from port1 and port2 to port3 in 10G speed in queue 0, and port3 will be in congestion.

For the multicast flow,If flow control is enabled on port1 and port2 and configure static threshold,the packets also perhaps will be dropped in port 3 egress queue,because at the egress shared-ratio is small and ingress can't meet condition of sending pause frame.

So,if users exist this environment,in the this condition,we suggest users configure dynamic mode. port1 and port2 will send out pause frame before port3 queue limit is reached, and absorb burst packets to avoid packet drop.

What's more,if pause frame are not be responsed,uc traffic will be discarded on ingress port,whether mc traffic are discarded on egress port.

Note:

1.support buffer managment platforms:

trident2	trident2 plus	tomahawk(per xpe)	triumph3	trident

2.Unicast queue traffic

push_mpls,push_l2mpls,gre,l2gre,vxlan,multitable flow,TTP unicast flow.

3.platform 4610,6248

multicast queue can absorb 266 cells,other platforms can absorb about 300 cells.

Configuring snmp

Pica8 support snmp from version 2.9.1 on ovs.

SNMP is short for Simple Network Management Protocol, and it is mainly used for monitoring features, data throughout, communication overload, errors and so on of network devices.

SNMP is composed of agent-side and server-side which contains three communication behaviors between them: get, set and trap. The communication process can be detailed roughly as follows: server sends requests (snmpget or snmpwalk) to agent and then agent will deal with the requests and reply to it. While agent will also send notification to server proactively when finding device status changed or errors occuring.What is more,one server-side can monitor multiple agent-sides and vice versa.

SNMP can not work without mibs which determine the available objects of a device. Every mib can be represented by a subtree and each node in the tree corresponds to one OID number which means one available variable in our device. Our SNMP currently mainly support public IF-MIB and private mibs (pica_private_mib.txt and pica_private_trap_mib.txt) which are defined by ourselves. The specified contents of our defined private mibs can be referred in this site: Pica8 Private MIB

1.start snmp on ovs

```
admin@XorPlus$sudo picos_boot
Configure the default system start-up options:
 (Select key 3 if no change)
    [1]  PicOS L2/L3   * default
    [2]  PicOS Open vSwitch/OpenFlow
    [3]  No start-up change
Enter your choice (1,2,3):2
PicOS Open vSwitch/OpenFlow is selected.
Configure the IP of management interface:
    [1] DHCP
    [2] Static IP
Enter your choice(1,2):1
Start OVS web user interface?(y|n)[n]:y
Start OVS network snmp?(y|n)[n]:y
Please restart the PicOS service
admin@XorPlus$sudo systemctl restart picos
```

2.command

We enable ovs snmp to update device data and enable trap using following command.

1)Enable snmp:

```
admin@PicOS-OVS$ovs-vsctl set-snmp-enable true
admin@PicOS-OVS$ovs-vsctl show-snmp
  snmp is enabled
admin@PicOS-OVS$
```

2)Configure snmp community name:

```
admin@PICOS-OVS:~$ ovs-vsctl set-snmp-community-name  pica8
```

Snmp community name default value is public, following command reproduce default value.

```
admin@PicOS-OVS$ ovs-vsctl set-snmp-community-name
```

3)Change trap destinations:

```
admin@PicOS-OVS$ovs-vsctl  show-snmp-trap-targets
snmp trap target is default: l27.0.0.1
admin@PicOS-OVS$
```

Note:default snmp trap target is 127.0.0.1,and we can use following command to change it.

```
admin@PicOS-OVS$ovs-vsctl set-snmp-trap-targets 10.10.50.234
```

Reproduce default snmp trap target:

```
admin@PicOS-OVS$ovs-vsctl set-snmp-trap-targets
```

3.Snmp

Snmpwalk and snmpget:

Both linux console and window SNMP tool can get device data. Following are results from 10.10.51.194:

```
pica8@pica8:~$ snmpwalk -v 2c -c public 10.10.51.157 1.3.6.1.4.1.35098.1.1
iso.3.6.1.4.1.35098.1.1.0 = INTEGER: 8
pica8@pica8:~$
pica8@pica8:~$ snmpget -v 2c -c public 10.10.51.157 1.3.6.1.4.1.35098.1.1.0
iso.3.6.1.4.1.35098.1.1.0 = INTEGER: 8
pica8@pica8:~$
```

Note: Generally using snmpwalk for snmp data is safer and convinient.On one hand, you can get all data of a table or a group for requesting once by snmpwalk. But snmpget need many times. On the other hand,for snmpget,you need use leaf node of a mib plus index as OID number, while snmpwalk do not. The root difference between them lies in that snmpget can only access a leaf node for one request, but snmpwalk can access a root node instead. For example, cpuUsage OID is 1.3.6.1.4.1.35098.1.1. if you use snmpget,you must access it like this:

snmpget -v 2c -c public 10.10.51.145 1.3.6.1.4.1.35098.1.1.0

Trap notification:

You can use window snmp tools to save the notification results.

4.Tap on snmp:

> ⚠ Following configure only used flows which added by web tapping.

As we know, OVS can be configured through its build-in commands, But web looks like more convenient and intuitive.So we develop web to configure OVS in tap units. One tap corresponds a flow in OVS which contains a set of in_ports(flow inports), a set of filters(flow match), a hash type for out-ports(group type + lag hash) and a set of out-ports(make up a group for flow output). One user can create many different taps to control OVS work. Snmp can work as a way of checking the tap configuration other than physical device status and trap.

Oids about tap:

Global lag hash oid:

glLagHashFields OID 1.3.6.1.4.1.35098.3.1

Tap table field oid:

tapEntry OID 1.3.6.1.4.1.35098.3.2.1

tapPrior OID 1.3.6.1.4.1.35098.3.2.1.1

inPortName OID 1.3.6.1.4.1.35098.3.2.1.2

f-srcMac OID 1.3.6.1.4.1.35098.3.2.1.3

f-dstMac OID 1.3.6.1.4.1.35098.3.2.1.4

f-srcIp OID 1.3.6.1.4.1.35098.3.2.1.5

f-dstIp OID 1.3.6.1.4.1.35098.3.2.1.6

f-dlType OID 1.3.6.1.4.1.35098.3.2.1.7

f-nwProto OID 1.3.6.1.4.1.35098.3.2.1.8

f-dlVlan OID 1.3.6.1.4.1.35098.3.2.1.9

f-tcpSrc OID 1.3.6.1.4.1.35098.3.2.1.10

f-tcpDst OID 1.3.6.1.4.1.35098.3.2.1.11

f-udpSrc OID 1.3.6.1.4.1.35098.3.2.1.12

f-udpDst OID 1.3.6.1.4.1.35098.3.2.1.13

f-nwTos OID 1.3.6.1.4.1.35098.3.2.1.14

f-vlanPcp OID 1.3.6.1.4.1.35098.3.2.1.15

a-mod-srcMac OID 1.3.6.1.4.1.35098.3.2.1.16

a-mod-dstMac OID 1.3.6.1.4.1.35098.3.2.1.17

a-mod-vlanVid OID 1.3.6.1.4.1.35098.3.2.1.18

a-mod-vlanPcp OID 1.3.6.1.4.1.35098.3.2.1.19

a-pushVlan OID 1.3.6.1.4.1.35098.3.2.1.20

a-popVlan OID 1.3.6.1.4.1.35098.3.2.1.21

portGroupType OID 1.3.6.1.4.1.35098.3.2.1.22

outPortName OID 1.3.6.1.4.1.35098.3.2.1.23

mirror table oids:

mirrorEntry OID 1.3.6.1.4.1.35098.3.3.1

mirrorIndex OID 1.3.6.1.4.1.35098.3.3.1.1

mirrorName OID 1.3.6.1.4.1.35098.3.3.1.2

srcPort OID 1.3.6.1.4.1.35098.3.3.1.3

dstPort OID 1.3.6.1.4.1.35098.3.3.1.4

outputPort OID 1.3.6.1.4.1.35098.3.3.1.5

Example:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=53, cookie=0x3, duration=1823.837s, table=0, n_packets=n/a, n_bytes=0, priority=3,in_port=130 actions=outp
 flow_id=54, cookie=0xfffc, duration=1823.829s, table=0, n_packets=n/a, n_bytes=0, priority=65532,in_port=133,dl_s
admin@PicOS-OVS$
admin@PicOS-OVS$sudo su
root@PicOS-OVS$

root@PicOS-OVS$ovs-vsctl list mirror
_uuid               : 1080b149-740e-414f-8054-3250f041cf7e
external_ids        : {}
name                : "M1"
output_port         : ef639e9a-a215-4a33-9c04-9e463137c91f
output_vlan         : []
select_all          : false
select_dst_port     : [05360726-9dac-4cd0-9a1d-7adf9e9d9026, d090f287-e96b-44a5-ade3-a30f662c075e]
select_src_port     : [11568bd4-0456-4e8d-b294-95ae94d8fb3a, 52c4e38a-dac7-425f-ba64-701122491f34, 5b77ec3e-5fdd-4
select_vlan         : []
statistics          : {}
root@PicOS-OVS$
```

The results from 10.10.51.194:

```
pica8@pica8:~$snmpwalk -v 2c -c public 10.10.51.174 1.3.6.1.4.1.35098.3.2.1
NPB-PRIVATE-MIB::tapPrior.3 = INTEGER: 3
NPB-PRIVATE-MIB::tapPrior.65532 = INTEGER: 65532
NPB-PRIVATE-MIB::inPortName.3 = STRING: "he-1/1/2"
NPB-PRIVATE-MIB::inPortName.65532 = STRING: "he-1/1/5"
NPB-PRIVATE-MIB::f-srcMac.65532 = STRING: "11:11:11:11:11:11"
NPB-PRIVATE-MIB::portGroupType.3 = STRING: "physical"
NPB-PRIVATE-MIB::outPortName.3 = STRING: "he-1/1/9"
pica8@pica8:~$
pica8@pica8:~$snmpwalk -v 2c -c public 10.10.51.174 1.3.6.1.4.1.35098.3.3.1
NPB-PRIVATE-MIB::mirrorIndex.1 = INTEGER: 1
NPB-PRIVATE-MIB::mirrorName.1 = STRING: "M1"
NPB-PRIVATE-MIB::rxPort.1 = STRING: "he-1/1/3 he-1/1/4 he-1/1/17 he-1/1/18"
NPB-PRIVATE-MIB::txPort.1 = STRING: "he-1/1/1 he-1/1/2"
NPB-PRIVATE-MIB::outputPort.1 = STRING: "he-1/1/19"
pica8@pica8:~$
```

5.Snmp trap

Pica8 added some private and trap MIBs listed below:

1.link up: OID: 1.3.6.1.6.3.1.1.5.4(physical port and lag port)

link down:OID:1.3.6.1.6.3.1.1.5.3(physical port and lag port)

2.sfpTraps: 1.3.6.1.4.1.35098.21.2

1)sfpPlugin: 1.3.6.1.4.1.35098.21.2.1

2)sfpPlugout: 1.3.6.1.4.1.35098.21.2.2

3,Warm start : OID:1.3.6.1.6.3.1.1.5.2

4,Cold start: OID:1.3.6.1.6.3.1.1.5.1

5,Rpsu traps: oid: 1.3.6.1.4.1.35098.21.1

1)rpsuPlugIn：1.3.6.1.4.1.35098.21.1.2

2)rpsuPlugOut：1.3.6.1.4.1.35098.21.1.3

3)rpsuFanFailed: 1.3.6.1.4.1.35098.21.1.4

4)rpsuFanRecovery: 1.3.6.1.4.1.35098.21.1.7

5)rpsuStatusChangePowerOff:1.3.6.1.4.1.35098.21.1.5

6)rpsuStatusChangePowerOn:1.3.6.1.4.1.35098.21.1.6

6,Fan traps: oid: 1.3.6.1.4.1.35098.21.1

1)switchFanFailed: 1.3.6.1.4.1.35098.21.3.1

2)switchFanRecovery: 1.3.6.1.4.1.35098.21.3.4

Note:

From 2.10.0,Pica8 support log info and trap message about fan and psu.
1) Fan log: fan fail, fan recovery.
2) Fan trap: fan fail, fan recovery.
3) Psu log: plugin,plugout,psu fail,psu recovery,psu power on,psu power off,psu status change.
4) Psu trap: plugin,plugout,psu fail,psu recovery,psu power on,psu power off.

Configuring/Enabling SNMPv3

- Description
- Procedure
- Commands
  - SNMPv3 User
  - SNMP MIB View
  - SNMP Group

Description

authentication-key and privacy-key of the user should not below the length requirements of the USM (min=8).

Security-level:If you create a snmpv3 user without adding to any group,then snmpwalk will use user's permission;If the user add to a group with a mib-view,then snmpwalk will use group's permission,and also support to use user's permission to snmpwalk when user's permission is higher then group's permission.

Procedure

Firstly, need to select 'Y' when "Start OVS network snmp?(y|n)[n]:'

Secondly, should execute "ovs-vsctl set-snmp-enable true" to enable snmp

At last, you can configure snmpv3 commands such as snmp-mib-view,snmp-group,snmpv3_user,etc in your test environment.

need to enable snmp(ovs-vsctl set-snmp-enable true) to make snmpv3 works.

Commands

SNMPv3 User

ovs-vsctl set-snmpv3-user username=user1 **readonly**=true **authentication-mode=**MD5 **authentication-key**=pica8123 **privacy-mode**=DES **privacy-key**=11111111

----------Use this command to create or update a user.

ovs-vsctl list snmpv3-user

ovs-vsctl list snmpv3_user

---------- Use these commands to check the user

ovs-vsctl **destroy** snmpv3-user user1

ovs-vsctl **destroy** snmpv3_user user1

---------- Use these commands to delete the user

Note:Of course, privacy-mode and privacy-key, authentication_key are optional, but authentication-mode is mandatory. authentication_key and privacy_key are empty without setting them.

Readonly:true or false, "true" means using rouser,"false" means rwuser。

authentication_mode: MD5, SHA

privacy_mode: DES, AES, AES128

SNMP MIB View

ovs-vsctl set-snmp-mib-view name=view1 subtree=1.3.6.1.2.1.1.2.0 type=included mask=ff

---------- Use this command to create a mib-view

ovs-vsctl list snmp-mib-view

---------- Use this command to check a mib-view

admin@PICOS-OVS:/pica/core$ ovs-vsctl list snmp-mib-view

_uuid : 0f1fc049-c9c6-4386-8824-06c524b208b5

name : all

nodes : [505cd0c9-2dde-442e-b91f-798954f21635]

ovs-vsctl destroy snmp-mib-view view1

ovs-vsctl destroy snmp_mib_view view1

---------- Use these commands to delete a mib-view,but if the view is used in group,then failed to destroy it.

ovs-vsctl add-snmp-mib-view ...

---------- Use this command to append the parameters to the same view,parameters are the same with set-snmp-mib-view

ovs-vsctl set view_node $uuid subtree=… mask=…

---------- Use this command to modify subtree or mask individually

SNMP Group

ovs-vsctl set-snmp-group name=group1 users=user1,user2 security-level=AuthPriv read-view=view1 write-view=view1 notify-view=view1

---------- Use this command to create a group and add user and view to the group

security-level:

AuthPriv

AuthNoPriv

NoAuthNoPriv

ovs-vsctl add snmp-group group1 users $uuid

---------- Use this command to append a user to a group ,uuid is the user's uuid

ovs-vsctl list snmp-group

ovs-vsctl list snmp_group

---------- Use these commands to check the group

ovs-vsctl **destroy** snmp-group group1

ovs-vsctl **destroy** snmp_group group1

---------- Use these commands to destroy the group

4)check all the snmpv3 configurations

ovs-appctl snmp/show-v3-config

check the validation of above configurations

you can check if the configurations works or not through snmpwalk/snmpset

eg:

snmpwalk -v 3 -u user1 -a MD5 -A 11111111 -x DES -X 11111111 -l authPriv 10.10.51.165 1.3.6.1.2.1.1.2.0

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.35098.1.13

Configuring Precision Time Protocol

PTP introduction

From version 2.9.2,Pica8 switch support PTP(Precision Time Protocol).

On a modern communications network, most telecommunications services require that the frequency offset or time difference between devices be within an acceptable range. To meet this requirement, network clock synchronization must be implemented.

Network clock synchronization includes phase synchronization and frequency synchronization.

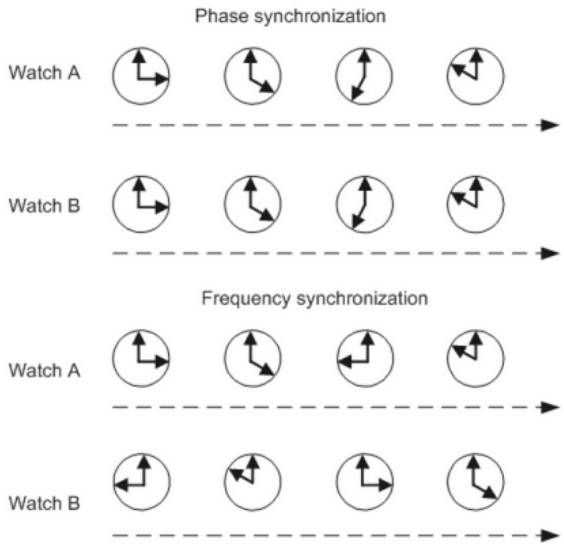
Phase synchronization

Phase synchronization, also called time synchronization, refers to the consistency of both frequencies and phases between signals. That is, the phase difference between signals is always 0.

Frequency synchronization

Frequency synchronization refers to constant phase difference between signals. It ensures that signals are sent or received at the same rate at a moment so that all devices on the communications network operate at the same rate.

Figure 1 Difference between time synchronization and frequency synchronization



PTP (Precision Time Protocol) is a time synchronization protocol, which itself is only used for high-precision time synchronization between devices, but can also be used to synchronize the frequency between devices. Compared to the existing time synchronization mechanism, PTP has the following advantages:

1.Compared to NTP (Network Time Protocol), PTP can meet the more accurate time synchronization requirements, NTP generally can only achieve sub-second time synchronization accuracy, and PTP can reach sub-microsecond.

2.Compared to GPS (Global Positioning System), PTP has lower construction and maintenance costs, and because it can get rid of the dependence on GPS, it has special meaning in national security.

Basic concepts

PTP domain

A PTP domain is a logical grouping of clocks that synchronize to each other using the protocol IEEE 1588v2, but that are not necessarily synchronized to clocks in another domain. Each PTP domain is an independent PTP clock synchronization system and has only one clock source.

Clock node

Clock nodes are nodes in a PTP domain. PTP defines the following types of clock nodes:

1.Ordinary clock (OC) device: provides only one physical port to participate in time synchronization in a PTP domain. An OC device uses this port to synchronize time with an upstream device or to send a downstream device.

2.Boundary clock (BC) device: provides two or more physical ports to participate in time synchronization in a PTP domain. One port synchronizes time with an upstream device, and the others send the time to downstream devices. A clock node is also a BC device if it functions as the clock source and sends time to downstream devices through multiple PTP ports.

3.Transparent clock (TC) device: forwards PTP messages between its PTP ports and measures the link delay of the messages. Different from an OC device and a BC device, a TC device does not synchronize time with other devices through ports.

- E2ETC (End-to-End Transparent Clock): forwards packets of non-P2P (Peer-to-Peer, point-to-point) types directly on the network and participates in the calculation of the entire link Time.

E2ETC calculate the residence time of the device, which is the time it takes the event message from ingress port to egress port, then add the calculated residence time to the correctionfield of the event message.

- P2PTC (Peer-to-Peer Transparent Clock): forwards only Sync messages, Follow_Up messages and Announce messages, and terminates other PTP packets. It is involved in calculating the entire link on the entire link. The delay of a link.

PTP port

A PTP port is a port running PTP. PTP ports are classified into the following types based on roles:

1.Master port: The port is the source of time on the path served by the port, located on a BC or OC device.

2.Slave port: The port synchronizes to the device on the path with the port that is in the MASTER state, is located on a BC or OC device.

3.Passive port: The port is not the master on the path nor does it synchronize to a master.is an idle port on a BC device and does not receive or send synchronization clock signals.

Master-slave hierarchy

Nodes in a PTP domain establish the master-slave hierarchy for clock synchronization. Master nodes send synchronization clock signals, while slave nodes receive synchronization clock signals. A device may receive synchronization clock signals from an upstream node and then send the synchronization clock signals to a downstream device.

If two clock nodes synchronize time with each other:

1.The node that sends synchronization clock signals is the master node, and the node that receives synchronization clock signals is the slave node.

2.The clock on the master node is the master clock, and the clock on the slave node is the slave clock.

3.The port that sends synchronization clock signals is the master port, and the port that receives synchronization clock signals is the slave port.

Grandmaster clock

All clock nodes in a PTP domain are organized into the master-slave hierarchy. The grandmaster clock (GMC) is at the top of the hierarchy and is the reference clock in the PTP domain. Clock nodes exchange PTP messages to synchronize the time of the GMC to the entire PTP domain. Therefore, the GMC is also called the clock source. The GMC can be statically configured or dynamically elected through the best master clock (BMC) algorithm.

PTP message

Nodes exchange PTP messages to establish the master-slave hierarchy and implement time and frequency synchronization. PTP messages are classified into event messages and general messages depending on timestamps:

1.Event message: is tagged with a timestamp when reaching or leaving a port. PTP devices calculate the link delay based on the timestamps carried in event messages. Event messages include Sync, Delay_Req, Pdelay_Req, and Pdelay_Resp messages.

2.General message: is used to establish master-slave hierarchy, and to request and send time information. General messages are not tagged with timestamps. General messages include Announce, Follow_Up, Delay_Resp, Pdelay_Resp_Follow_Up, Management, and Signaling messages. Currently, devices do not support Management and Signaling messages.

> ⚠ The product supports only E2ETC function, and uses Sync, Delay_Req and Delay_Resp PTP messages.

Flow chart of delay Request-Response Mechanism

Figure 2 shows the process of calculating the average link delay and time offset between the master and slave devices using the E2E mechanism.

Figure 2 Delay request-response mechanism

1.The master sends a Sync message to the slave and notes the time t1 at which it was sent..

2.The slave receives the Sync message and notes the time of reception t2.

3.The master conveys to the slave the timestamp t1 by:

a) Embedding the timestamp t1 in the Sync message. This requires some sort of hardware

processing for highest accuracy and precision.

b) Embedding the timestamp t1 in a Follow_Up message.

4.The slave sends a Delay_Req message to the master and notes the time t3 at which it was sent.

5.The master receives the Delay_Req message and notes the time of reception t4.

The master conveys to the slave the timestamp t4 by embedding it in a Delay_Resp message.

By exchanging messages with the master device, the slave device obtains t1, t2, t3, and t4, and calculates the average link delay and time offset between the master and slave devices. Then the slave device can adjust the local time according to the calculated time offset to synchronize with the master device. The formulas for calculating the link delay and time offset are as follows:

Average link delay = [(t4- t1) - (t3- t2)]/2

Offset = [(t2- t1) + (t3- t4)]/2

Product Support

The table below shows the model and the corresponding switch ASIC that support the PTP function, others do not support.

Switch ASIC		Model
Helix4	BCM56342	as4610-30t
		as4610_30p
	BCM56340	as4610_54t
		as4610_54p

Trident2	BCM56850	pronto5101
		pronto5401
		as6701-32x
		as6712-32x
	BCM56854	pronto5101
		as5712-54x
		s4048
		arctica4806xp
Trident2Plus	BCM56864	as5812-54t
		as5812-54x
Tomahawk	BCM56960	dcs7032q28
		z9100
		as7312
		as7712-32x

PTP configuration

Configure the device interface as the E2ETC node type, enable the PTP function on the interface, and implement the device to forward the PTP packets directly.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:ptp-mode=e2etransparent
```

By default, PTP is disabled on an interface.

Disable ptp mode on the interface:

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:ptp-mode=none
```

- The PTP function can only be configured on the physical interface.
- On the TC device, PTP must be enabled on all the interfaces that receive and send PTP messages. Otherwise, the PTP function will work inproperly.

Configuration example

Configure the port te-1/1/1 that receiving PTP messages and the port te-1/1/2 that sends PTP packets as E2ETC node.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:ptp-mode=e2etransparent
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:ptp-mode=e2etransparent
```

Add flow.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:2
```

Result:ptp message are forwarded normally and te-1/1/2 receive ptp packets with correction.

Configuring Tunneling

Configuring GRE

PicOS OVS supports IP GRE tunneling.

The port ranges in PicOS are as follows:

Port Type	Port Number
GRE	3073-4095

GRE ON Physical PORT

Creating a GRE tunnel

```
root@PicOS-OVS# ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.60.10 opt
```

If the user wants to create a GRE tunnel, the user will need to configure a GRE tunnel along with two flows, which are used for sending traffic to the GRE and sending output from the GRE respectively.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:3073
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=3073,actions=mod_dl_src:00:11:11:11:11:11,mod_dl_dst:00:33:33:33:33
```

The GRE port number starts from 3073, which is the port number of GRE1. The first flow in the example above, is configured so that all traffic from port ge-1/1/1 will be sent to the GRE tunnel, whose port number is 3073. The second flow is configured so that all of the traffic coming out from the GRE tunnel will be forwarded to port ge-1/1/1 and the source MAC address modified to the switch's MAC address and the destination MAC address to the MAC address of the internal target. (If user doesn't specify the dl_src in the action of second flow, the src mac will be the switch's mac, but the dst mac must be specified.)

Description

1. br0: bridge name
2. remote_ip=10.10.60.10: the IP address of the peer GRE tunnel interface; this IP address will be the destination IP of the encapsulated GRE packets
3. local_ip=10.10.61.10: the IP address of this GRE tunnel interface; this IP address will be the source IP of the encapsulated GRE packets
4. src_mac=00:11:11:11:11:11: the logical MAC address of the GRE tunnel interface; this MAC address will be the source MAC of the encapsulated GRE packets to next-hop
5. dst_mac=00:22:22:22:22:22: the next-hop MAC address; this MAC address will be the destination MAC the encapsulated GRE packets to next-hop
6. egress_port=ge-1/1/5: the output port of the encapsulated GRE packets

GRE ON LAG/LACP PORT

Static Lag and GRE Tunnel

Command:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:membe
admin@PicOS-OVS$ovs-vsctl -- set interface ae1 options:lag_type=static
admin@PicOS-OVS$ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:local_ip=10.10.60.10 optic
```

Flows:

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:3073
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=3073,actions=mod_dl_src:00:11:11:11:11:11,mod_dl_dst:00:33:33:33:33
```

LACP and GRE Tunnel

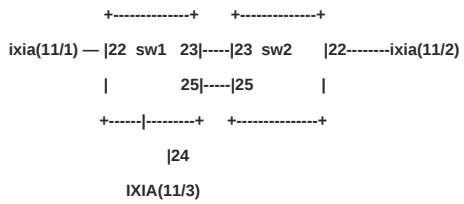
Command:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:membe
admin@PicOS-OVS$ovs-vsctl -- set interface ae1 options:lag_type=lacp
admin@PicOS-OVS$ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:local_ip=10.10.60.10 optic
```

Flows:

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:3073
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=3073,actions=mod_dl_src:00:11:11:11:11:11,mod_dl_dst:00:33:33:33:33
```

Example



SW1 CONFIG:

Step1: Create a bridge and add two ports (PX1,PX2,PX3)

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/22 vlan_mode=trunk tag=1 -- set interface ge-1/1/22 type=pica8
ovs-vsctl add-port br0 ge-1/1/23 vlan_mode=trunk tag=1 -- set interface ge-1/1/23 type=pica8
ovs-vsctl add-port br0 ge-1/1/25 vlan_mode=trunk tag=1 -- set interface ge-1/1/25 type=pica8
```

Step 2: Add static lag port and gre port

```
ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:members=ge-1/1/23,ge-
ovs-vsctl -- set interface ae1 options:lag_type=static
ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:local_ip=10.10.60.10 options:remote_ip=10
```

Step 3: Add flow

```
ovs-ofctl add-flow br0 in_port=22,actions=output:3073
ovs-ofctl add-flow br0 in_port=3073,actions=set_field:66:66:66:44:44:44-\>dl_dst,set_field:66:66:66:33:33:33-\>dl_
```

SW2 CONFIG:

Step1: Create a bridge and add two ports (PX1,PX2,PX3)

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/22 vlan_mode=trunk tag=1 -- set interface ge-1/1/22 type=pica8
ovs-vsctl add-port br0 ge-1/1/23 vlan_mode=trunk tag=1 -- set interface ge-1/1/23 type=pica8
ovs-vsctl add-port br0 ge-1/1/25 vlan_mode=trunk tag=1 -- set interface ge-1/1/25 type=pica8
```

Step 2: Add flow

```
ovs-ofctl add-flow br0 in_port=23,actions=output:22
ovs-ofctl add-flow br0 in_port=25,actions=output:22
```

SEND Packets

Step 4: Send ipv4 packets,check the result(limitation:the src mac and vlan of the packets must be the same with gre tunnel)

(1) send no changing packets to PX1,

Result:

then PX2 or PX3 will transmit all the encapsulated packets

check nw_dst=10.10.61.10,nw_src= 10.10.60.10,vlan=1012,src_mac=C8:0A:A9:04:49:1A ,dst_mac=C8:0A:A9:9E:14:A5

Check:

dst mac: C8 0A A9 9E 14 A5

src mac: C8 0A A9 04 49 1A

offset:12

vlan: 81 00 03F4

dst ip: 0A 0A 3D 0A

src ip: 0A 0A 3C 0A

(2) sending increasing src ip to PX1,(first enable hash mapping mode:ovs-vsctl -- set Interface ae1 options:hash-mapping=advance ovs-vsctl set-lag-advance-hash-mapping-fields nw_src)

Result:

```
then both PX2 and PX3 will transmit the encapsulated packets
check nw_dst=10.10.61.10,nw_src= 10.10.60.10,vlan=1012,src_mac=C8:0A:A9:04:49:1A ,dst_mac=C8:0A:A9:9E:14:A5
```

Then reconfigure sw2

Step1: Add static lag port and gre port

```
ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:members=ge-1/1/23,ge-
ovs-vsctl -- set interface ae1 options:lag_type=static
ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.60.10 options:local_ip=10
options:dst_mac=C8:0A:A9:04:49:1A options:egress_port=ae1
```

Step 2: Add flow

```
ovs-ofctl add-flow br0 in_port=22,actions=output:3073
ovs-ofctl add-flow br0 in_port=3073,actions=set_field:66:66:66:44:44:44-\>dl_dst,set_field:66:66:66:33:33:33-\>dl_
```

SEND Packets

(1) sending no changing packets to ge-1/1/22(SW1),

Result:

ge-1/1/22(SW2) will transmit the decapsulated packets.

check dl_src=66:66:66:33:33:33,dl_dst=66:66:66:44:44:44,vlan 1012

Configuring L2GRE

The port ranges in PicOS are as follows:

Port Type	Port Number
L2GRE	5121-6143

PicOS OVS support Layer 2 over Generic Routing Encapsulation (L2GRE); the port number of L2GRE ranges from 5121 to 6143. GRE is an encapsulated mechanism that encapsulates packet IPs; L2GRE is an encapsulated mechanism that encapsulates the entire packet.To resolve the problem that pushes the interface PVID to the untagged packets before encapsulation by the L2GRE header, use the command **ovs-vsctl set interface <interface> type=pica8 options:access-vport=true**. Like this, the untagged packets can be encapsulated by L2GRE header with no VLAN; that is, the PVID of ingress port. And the tagged packets are encapsulated by L2GRE header, the inner VLAN is the VLAN tag of the packets that are received by ingress port. See the example below.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.1
```

Description

1. br0: bridge name
2. remote_ip=10.10.61.10: the IP address of the peer L2GRE tunnel interface; this IP address will be the destination IP of the encapsulated L2GRE packets
3. local_ip=10.10.60.10: the IP address of this L2GRE tunnel interface; this IP address will be the source IP of the encapsulated L2GRE packets
4. src_mac==C8:0A:A9:9E:49:1A: the logical MAC address of the L2GRE tunnel interface; this MAC address will be the source MAC of the encapsulated L2GRE packets to next-hop
5. dst_mac=C8:0A:A9:9E:14:A5: the next-hop MAC address; this MAC address will be the destination MAC the encapsulated L2GRE packets to next-hop
6. egress_port=te-1/1/12: the output port of the encapsulated L2GRE packets
7. l2gre_key=1234:the key value of L2GRE tunnel,different tunnel has different key.
8. vlan=1:the vlan of L2GRE tunnel.this vlan will be pop or not according to the pvid of the egress port.

Examples

push one L2GRE header

topology



Creating a L2GRE tunnel

(1) create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

(2) add ports to br0.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/11 vlan_mode=trunk tag=1 -- set Interface te-1/1/11 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/12 vlan_mode=trunk tag=1 -- set Interface te-1/1/12 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.1
```

User must configure a flow if user wants to send packets to a L2GRE port. And port number is 5121 for l2gre1 tunnel, different L2GRE tunnels must have different l2gre_key.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:5121
```

Send packets (ARP, L2/L3 packets) to te-1/1/11,then packets are encapsulated by L2GRE header. when the VLAN tag of Layer 2 GRE tunnel is the same with native VLAN-ID of output port, L2GRE VLAN of the packets are stripped when forwarded by egress port. When the VLAN tag of L2GRE tunnel is different from native VLAN-ID \output port, L2GRE VLAN of the packets are not stripped when forwarded by egress port.

strip L2GRE tunnel



configuration

configure the L2GRE tunnels named l2gre1 on te-1/1/12 of swa and l2gre2 on te-1/1/12 of swb.

swa:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.
```

swb:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.60.
```

User must add the two flows below if user wants to push L2GRE header on te-1/1/12 of swa and strip the Layer 2 GRE header on te-1/1/12 of swb.

Swa:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:5121
```

swb:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=5121,actions=output:1
```

te-1/1/11 of swb will receive the original packets (the contents of packets are the same with packets that te-1/1/11 of swa received).

configure two L2GRE tunnels on one physical port



Configuration

Configure two L2GRE tunnels on both te-1/1/12(l2gre1,l2gre2) and te-1/1/13(l2gre1,l2gre2). These two tunnels have different IP and l2gre_key so user must configure some flows.

Sw1:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.60.
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre2 -- set Interface l2gre2 type=pica8_l2gre options:remote_ip="10.10.61
```

flows in sw1,

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:66:66:66:66:66,actions=output:5121
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:66:66:66:66:67,actions=output:5122
```

sw2:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre2 -- set Interface l2gre2 type=pica8_l2gre options:remote_ip=10.10.60.
```

flows in sw2

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=5121,dl_dst=22:66:66:66:66:66,actions=output:4
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=5122,dl_dst=22:66:66:66:66:67,actions=output:5
```

send packets to te-1/1/11,different packets will go to different L2GRE tunnels. When they are stripped L2GRE header on te-1/1/13,they are forwarded to a different port.

Length of l2gre_key

In pica8 switch, the length of l2gre_key can be 16bit, 20bit, 24bit or 32bit; 24 bit is the default value.



configuration

configure the L2GRE tunnel on te-1/1/12 .

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.
```

Add a flow to switch

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:5121
```

This key of L2GRE tunnel is 1234 here in decimal, 4d2 in hex. The default value of Layer 2 GRE key is 24, so the value of GRE key of packets is 0x004d2000. When user sets the l2gre_key value to 16 using the command **ovs-vsctl set-l2gre-key-length 16,** the value of the GRE key of packet is 0x04d20000. When user sets the l2gre_key value to 20 using the command **ovs-vsctl set-l2gre-key-length 24,** the value of GRE key packet is 0x0004d200. When user sets the l2gre_key value to 32 using the command **ovs-vsctl set-l2gre-key-length 32,** the value of GRE key packet is 0x000004d2.

Collaboration between nvgre and VXLAN



Configuration

configure the L2GRE tunnel and VXLAN tunnel on te-1/1/12 and te-1/1/13.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.60.1
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.1
```

Flows in Switches

sw1:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:23,actions=output:4097
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=output:5121
```

sw2:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=5122,dl_dst=22:22:22:22:22:22,actions=output:4
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=4098,dl_dst=22:22:22:22:22:23,actions=output:5
```

te-1/1/14 should receive the de-capsulated packets with src_mac 22:22:22:22:22:22, te-1/1/15 should receive the de-capsulated packets with src_mac 22:22:22:22:22:23.That is to say VXLAN and L2GRE do not affect each other.

Configuring L2MPLS

> **INFO**
> 1.set mac actions should not be added before push_l2mpls

PUSH L2 MPLS

Pushing an L2 MPLS with one label:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=17,ip,dl_vlan=11,actions=push_l2mpls:0x8847,set_field:22:11:11:11:1
```

Pushing an L2MPLS with two labels:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=17,ip,dl_vlan=11,actions=push_l2mpls:0x8847,set_field:22:11:11:11:1
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=17,dl_type=0x8847,dl_vlan=11,actions=push_mpls:0x8847,set_field:22:
```

SWAP L2 MPLS Label

In the following configuration example, specify a flow which has two labels, and in this situation user wants to swap the outer label. The output flow is L2MPLS packet with outer label 30 and inner label 20.

```
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=18,dl_type=0x8847,dl_dst=22:00:00:00:00:01,dl_vlan=11,mpls_label=16
```

POP L2MPLS Label

Popping an MPLS Label of the flow:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=17,dl_vlan=11,dl_dst=22:00:00:00:00:01,mpls,mpls_label=16,actions=p
```

Popping one MPLS label for flows with two MPLS labels:

Two labels then pop one outer label.

```
root@PicOS-OVS$ovs-ofctl add-flow br0 "in_port=17,dl_vlan=11,dl_dst=22:00:00:00:00:01,mpls,mpls_label=16,mpls_label
```

Popping two MPLS labels for flows with two MPLS lables

In the following configuration, specify a flow which has two labels to pop. The output flow is IP packet. Configure two pop entries to pop the flow.

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=17,dl_vlan=11,dl_dst=22:00:00:00:00:01,mpls,mpls_label=16,mpls_label
```

PUSH L2MPLS Label and VLAN

Pushing one L2MPLS label and one VLAN:

In the following configuration, specify flows to push one L2MPLS label and one VLAN.

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=17,ip,actions=push_l2mpls:0x8847,set_field:22:22:22:22:22:22->dl_ds
root@PicOS-OVS#ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,dl_dst=22:22:22:22:22:22,mpls_label=66
```

Pushing two L2MPLS Labels and one VLAN:

In the following configuration, specify flows to push two MPLS labels and one VLAN.

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=17,ip,actions=push_l2mpls:0x8847,set_field:22:11:11:11:11:10->dl_ds
```

Pushing One MPLS Label and Pop One VLAN

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=18,dl_type=0x8847,mpls_label=30,dl_dst=22:22:22:22:22:22,dl_src=44:4
```

Pushing One L2MPLS Label and Pop One VLAN

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=18,dl_vlan=100,actions=push_L2mpls:0x8847,set_field:22:22:22:22:22:2
```

Pushing Two L2MPLS Headers

```
root@PicOS-OVS#ovs-ofctl add-flow br0 "in_port=18,dl_type=0x8847,actions=push_l2mpls:0x8847,set_field:22:00:00:00:0
```

Configuring Inner VLAN

Push L2MPLS, push one inner VLAN:

```
ovs-ofctl add-flow br0 "in_port=17,ip,actions=push_vlan:0x8100,set_field:8->vlan_vid,push_l2mpls:0x8847,set_field:2

ovs-ofctl add-flow br0 "in_port=17,dl_vlan=2,ip,actions=push_vlan:0x8100,set_field:8->vlan_vid,push_l2mpls:0x8847,s
```

Push L2MPLS, modify inner VLAN:

```
ovs-ofctl add-flow br0 "in_port=17,ip,actions=set_field:8->vlan_vid,push_l2mpls:0x8847,set_mpls_ttl:64,set_field:22

ovs-ofctl add-flow br0 "in_port=17,dl_vlan=2,ip,actions=set_field:8->vlan_vid,push_l2mpls:0x8847,set_mpls_ttl:64,se
```

Push L2MPLS, pop inner VLAN:

```
ovs-ofctl add-flow br0 "in_port=17,dl_vlan=2,ip,actions=pop_vlan,push_l2mpls:0x8847,set_mpls_ttl:64,set_field:22:22
```

Pop inner VLAN after pop L2MPLS:

```
ovs-ofctl add-flow br0 "in_port=17,dl_vlan=11,dl_dst=22:22:22:22:22:22,mpls,mpls_label=1000,actions=pop_l2mpls,pop_
```

Modify inner VLAN after popping L2MPLS:

```
ovs-ofctl add-flow br0 "in_port=18,dl_vlan=11,dl_dst=22:22:22:22:22:22,mpls,mpls_label=16,mpls_label2=20,actions=po
```

ⓘ The L2MPLS packet must encapsulate outer VLAN and not be PVID, the original packets must encapsulate the VLAN tag.

Push inner VLAN after popping L2MPLS:

```
ovs-ofctl add-flow br0
"in_port=17,dl_vlan=11,dl_dst=22:22:22:22:22:22,mpls,mpls_label=1000,actions=pop_l2mpls,push_vlan:0x8100,set_field
```

ⓘ The L2MPLS packet must encapsulate outer VLAN and not be PVID, the original packets shouldn't encapsulate VLAN tag.

Configuring MPLS

The basic MPLS actions are Push, Swap and Pop. Beginning with PicOS 2.4, user does not need to set the ***eth_src*** in actions during Push MPLS. The packet **src_mac** pushes the MPLS to the MAC address of this switch.

- User can add flows to modify and copy the MPLS TTL and IP TTL.
- User can push/pop 2 MPLS labels per flow.

> Every un-tagged packet is tagged with the default VLAN-ID before Push, Pop and Swap.

Hardware or Software based Forwarding

The flow is pre-installed in hardware if there is enough information on the Flow to be processed by the ASIC.

Here is the minimal set of information required in flow match to process the packet on hardware only,**before version 2.8.1**:

If the Flow action is a POP : dl_dst, dl_vlan, mpls_lse
If the Flow action is a PUSH : dl_dst, dl_vlan, dl_type,mpls_lse (only being needed when dl_type is 0x8847 or 0x8848)
If the Flow action is a SWAP :dl_dst, dl_vlan, mpls_lse

Since version 2.8.1,configuration is changed,the minimal set on hardware only as shown below:

If the Flow action is a PUSH:
push mpls for ip packet: in_port,dl_vlan,dl_dst,dl_type
push mpls for mpls packet: in_port,dl_vlan,dl_dst,dl_type(mpls),mpls_label

If the Flow action is a SWAP: in_port,dl_vlan,dl_dst,dl_type(mpls),mpls_label

If the Flow action is a POP: in_port,dl_vlan,dl_dst,dl_type(mpls),mpls_label

> 1. There is one exception. If the action is "pop_mpls:0x8847" and matches enough fields (dl_dst,vlan_id,mpls_label), the flow becomes a direct flow (hardware only).
>
> 2. If the flow actions a push, flow match must include dl_type=0x0800/dl_type=0x86dd/dl_type=0x8847/dl_type=0x8848. If the flow match not include one of them, the flow entry cannot add.

If there is some information missing to process the packet, the flow becomes a "packet-driven" flow. This means that the first MPLS packet is sent to the CPU, which analyzes it and downloads a new flow on the hardware with the missing information to handle the packet in hardware. Following packets for this specific flow will then be handled by the hardware (ASIC) without reaching the Switch CPU.

PUSH MPLS

Pushing an MPLS Label

In the following configuration, user specifies a flow, which should match:
{ in_port=1,dl_type=0x0800, dl_dst=22:00:00:00:00:00,dl_vlan=1}
The action is to push an MPLS label (i.e. 10) and forward to port te-1/1/2
Note that MPLS TTL will copy from the IP header and decrease

Pushing two MPLS Labels

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_dst=22:00:00:00:00:00,dl_vlan=1,actions=push_mp
```

In the following configuration, specify a flow, which should match { in_port=1,dl_type=0x0800,dl_dst=22:00:00:00:00:00,dl_vlan=1}, the action is to push two labels (i.e. 10 and 20) /EXP/TTL and forward to port te-1/1/2

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_dst=22:00:00:00:00:00,dl_vlan=1,actions=push_mp
root@PicOS-OVS#
```

SWAP MPLS Label

Swapping MPLS Labels

In following configuration, user specifies a flow, which should match { in_port=1,dl_type=0x8847,dl_dst=22:00:00:00:00:00,dl_vlan=1,mpls_label=10}, the action is to swap label 10 with 20 and forward to port te-1/1/2

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,dl_dst=22:00:00:00:00:00,dl_vlan=1,mpls_label=10,a
root@PicOS-OVS#
```

POP MPLS Label

Popping an MPLS Label of the flow

In following configuration, specify a flow, which should match { in_port=1,dl_type=0x8847,dl_dst=22:00:00:00:00:00,dl_vlan=1,mpls_label=10}, the action is to pop MPLS label and forward to port te-1/1/2.
Note that MPLS TTL will be copied to IP header TTL and decremented by 1.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,dl_dst=22:00:00:00:00:00,dl_vlan=1,mpls_label=10,a
```

Popping one MPLS Label for flows with Two MPLS Labels

In the following configuration, specify a flow that has two MPLS labels (i.e. 10 and 20). The pop action is always popping the outer MPLS header. Note that the two label flow pops only one label, the output packet is also a MPLS packet. Thus, the "pop_mpls:0x8847" must be configured.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,dl_dst=22:00:00:00:00:00,dl_vlan=1,mpls_label=10,mp
```

Popping two MPLS Labels for flows with two MPLS Lables

In following configuration, specify a flow which has two labels to pop. The output flow is IP packet. Configure two pop entries to pop the flow.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,mpls_label=10,mpls_label2=20,dl_dst=22:00:00:00:00
```

notice :

if the action is pop_mpls:0x0800 to pop two mpls label, must have to match two mpls label.

PUSH MPLS Label and VLAN

Pushing one MPLS Label and one VLAN

In following configuration, specify flows to push one MPLS Label and one VLAN

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x0800,dl_vlan=2999,dl_dst=22:22:22:22:22:22,actions=push_mpls:0x8847,set_
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,dl_dst=22:22:22:22:22:22,mpls_label=66,actions=push_mp
```

Pushing two MPLS Labels and one VLAN

In following configuration, specify flows to push two mpls labels and one VLAN

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x0800,dl_vlan=2999,dl_dst=22:22:22:22:22:22,actions=push_mpls:0x8847,set_
```

POP One or Two MPLS Labels

In following configuration, specify flows which should match dl_type,dl_vlan and the MPLS label. The action is to pop one MPLS label and set a new src mac address. The first flow will pop one MPLS label and the second flow will pop two MPLS labels.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,mpls_label=111,dl_dst=22:22:22:22:22:22
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,mpls_label=111,actions=pop_mpls:0x0800
```

POP One or Two MPLS Labels and PUSH/SWITCH/POP VLAN

The following flow should match dl_type and dl_vlan, action is to pop one MPLS label and push one VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,mpls_label=111,dl_dst=22:22:22:22:22:22
```

The following flow should match dl_type and dl_vlan, with the action of popping two MPLS labels and pushing one VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,mpls_label=111,dl_dst=22:22:22:22:22:22
```

The following flow should match dl_type and dl_vlan and mpls label, and the action is to pop one MPLS labels and swap VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,dl_dst=22:22:22:22:22:22,actions=pop_mp
```

The following flow should match dl_type, the action is to pop two MPLS labels and pop VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,dl_dst=22:22:22:22:22:22,actions=pop_mp
```

PUSH MPLS and POP VLAN

In the following configuration, push MPLS label and pop VLAN have been supported. Following flow, the action is to push one MPLS label and pop one VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,dl_dst=22:22:22:22:22:22,actions=push_
```

SWITCH MPLS Labels and MOD/POP VLAN

Following flow, action is to push two MPLS labels and pop VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,dl_dst=22:22:22:22:22:22,actions=set_f
```

Following flow, action is to push two MPLS labels and mod VLAN.

```
ovs-ofctl add-flow br0 in_port=2,dl_type=0x8847,dl_vlan=2999,mpls_label=333,dl_dst=22:22:22:22:22:22,actions=set_f
```

NOTICE:

1. If flows match dl_vlan and the actions have push_vlan, then receives packets only carry the pushed vlan.
2. Hardware can't support pop_mpls and pop_vlan at the same time, and the packets can't forward with line-speed.
3. When actions don't appoint to modify dl_src, the src mac of received packets should be modified to bridge mac whatever for direct flows or packet-driven flow.
4. Push two mpls labels is supported, but push two vlans at the same time is not supported.
5. Hardware can't support push two vlan_header.

Match or Pop Reserved Mpls Label 0/2/3

From version 2.9.2, mpls support to match or pop reserved mpls label.

A value of 0 represents the "IPv4 Explicit NULL Label",this label value is only legal at the bottom of the label stack.

A value of 1 represents the "Router Alert Label", this label value is legal anywhere in the label stack except at the bottom.

A value of 2 represents the "IPv6 Explicit NULL Label",this label value is only legal at the bottom of the label stack.

A value of 3 represents the "Implicit NULL Label",this is a label that an LSR may assign and distribute, but which never actually appears in the encapsulation.

Example 1,match mpls label=0 and then pop_mpls:0x8847.

```
admin@PICOS-OVS$ovs-ofctl add-flow br0 in_port=1,mpls,mpls_label=0,dl_dst=22:22:22:22:22:22,dl_vlan=199,actions=pop
```

Send ipv4 packets with mpls_label=0 to match the flow, te-1/1/14 receive packets without mpls label.

Example 2,match mpls label2=0 and then pop_mpls:0x8847.

```
admin@PICOS-OVS$ovs-ofctl add-flow br0 in_port=1,mpls,mpls_label=100,mpls_label2=0,dl_dst=22:22:22:22:22:22,dl_vlan
```

Send ipv4 packets with mpls_label=100 and mpls_label2=0 to match the flow, te-1/1/14 receive packets with mpls_label=0.

Example 3,match mpls label=2 and then pop_mpls:0x8847.

```
admin@PICOS-OVS$ovs-ofctl add-flow br0 in_port=1,mpls,mpls_label=2,dl_dst=22:22:22:22:22:22,dl_vlan=199,actions=pop
```

Send ipv6 packets with mpls_label=2 to match the flow, te-1/1/14 receive packets without mpls label.

Example 4,match mpls label2=2 and then pop_mpls:0x0800.

```
admin@PICOS-OVS$ovs-ofctl add-flow br0 in_port=1,mpls,mpls_label=100,mpls_label2=2,dl_dst=22:22:22:22:22:22,dl_vlan
```

Send ipv6 packets with mpls_label=100 and mpls_label2=2 to match the flow, te-1/1/14 receive packets without mpls label.

1.It's not allowed to match/pop label 3. Additionally a label of 3 should not be included in MPLS encapsulation.
2.Platforms which support mpls:

3296 3780 3920 3922 3924 3930 5101 5401
* arctica4806xp as5712_54x as5812 as6701_32x as6712_32x as7712_32x
* dcs7032q28 es4654bf niagara2632xl niagara2948-6xl s4048 z9100 msh8920

2.Platforms which not support mpls:

3290 3295 as4610

Configuring PBB

PBB means Provider Backbone Bridge.

push

Push pbb_isid,eth_src,eth_dst

Outer src mac is set as 00:00:00:11:11:11, and dsc mac is set as 00:00:00:22:22:22,Vlan is set as 4094, pbb isid is set as 23.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=11,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22
```

Push pbb without pbb_isid,eth_src,eth_dst

Outer src mac is set as 22:11:11:11:11:11, and dsc mac is set as 22:22:22:22:22:22,Vlan is set as 4094, pbb isid is set as 0.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=11,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22
```

Push pbb_isid,eth_src,eth_dst for pbb packets

Outer src mac is set as 00:00:00:11:11:11, and dsc mac is set as 00:00:00:22:22:22,
Vlan is set as 4094, pbb isid is set as 21. (isid of primary pbb packet should not be 21)

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=11,dl_type=0x88e7,actions=push_pbb:0x88e7,set_field:21-\>pbb_isid,se
```

pop

Pop pbb packets tagged with vlan 1 (Primary pbb packets should be tagged with vlan 1) Pbb packets are popped.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=11,dl_type=0x88e7,dl_src=00:00:00:11:11:11,dl_dst=00:00:00:22:22:22
```

Pop pbb packets tagged with vlan 2000 (Primary pbb packets should be tagged with vlan 2000) Pbb packets are popped.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=11,dl_type=0x88e7,pbb_isid=23,dl_vlan=2000,dl_src=00:00:00:11:11:11
```

Important Things to Know

- Push pbb should be done with push_vlan,
- When do push pbb, primary src mac, and dst mac will be used if no config of eth_src , eth_dst
- Do push pbb for pbb packet, primary pbb isid should be not same as the push pb isid.
- When do pop pbb, primary packets should include vlan, and actions should include pop_vlan.
- All switches support pbb except P3290,P3295 and P4610.

Configuring QinQ

PicOS OVS supports QinQ. (3290,3295,3296 do not support set inner pcp)

Push tag, Push <tag:2000>

root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan:0x8100,set_field:2000-\>vlan_vid,output:2

Push <tag:2000 pcp:3>

root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan:0x8100,set_field:2000-\>vlan_vid,set_field:3-\>vlan_pcp,output:2

Push <tag:3000 tag:4094>

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan:0x8100,set_field:3000-\>vlan_vid,push_vlan:0x810(
```

Push <tag:3000 tag:4094 pcp:3>

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan:0x8100,set_field:3000-\>vlan_vid,push_vlan:0x810(
```

Push <tag:3000 pcp:3 tag:4094 pcp:7>

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan:0x8100,set_field:3000-\>vlan_vid,set_field:3-\>v1
```

Pop tag, Pop one header

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=pop_vlan,output:2
```

Pop two header

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=pop_vlan,pop_vlan,output:2
```

User can also use the strip_vlan to achieve pop VLAN tagged, for example:

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,priority=100,actions=strip_vlan,output:2
```

In hardware ASIC, implementation of "strip_vlan" is: change the packet's tag to "4095" and strip the vlan tag of 4095 in the egress. Thus, the above flow will be split into two flows in ingress and egress respectively, as follows:

Ingress "in_pot=1, priority=100, action=set_field:2000-\>vlan_vid"
Egress "in_pot=1, priority=100,action=strip_vlan,output:2"

In this case, maybe other traffic which matches the egress flow will be stripped vlan and forwarded to port-3. Users can install the other flow with higher priority to avoid this problem.

Hardware limitation of Pushing Two Tags
There is a limitation in pushing two tags; hardware ASIC can only identify two tags.

a. If primary packet is untagged, do two push_vlan (add tagA, tagB), output packets is tagged with two vlans. (tagA, tagB)

b. If primary packet is tagged with one vlan (tag0), do two push_vlan (add tagA, tagB), output packets is tagged with two vlans. (tag0, tagB),

c. If primary packet is tagged with more than one vlan (outer vlan is tag0), do two push_vlan (add tagA, tagB), output packets is tagged with vlans. (tag0 and other tag of primary packets, tagB),

d. For Platform 3290, 3295, 3296, 3297, 4804, these don't support modifying inner vlan pcp.

Configuring VXLAN

VXLAN port number of VXLAN ranges from 4097 to 5119. VXLAN mechanism is based on the limited number of VLANs(0-4094).VXLAN is used to provide more networks for switches or the host. To resolve the problem that pushing the interface' PVID to the untagged packets before encapsulated by the VXLAN header, the user must use this command "ovs-vsctl set interface <interface> type=pica8 options:access-vport=true ". Like this, the untagged packets can be encapsulated by VXLAN header with no VLAN that is pvid of ingress port. And the tagged packets are encapsulated by VXLAN header, the inner VLAN is the VLAN tag of packets that received by ingress port.

1, The port ranges in PicOS are as follows:

Port Type	Port Number
VXLAN	4097-5119

2.When the vxlan packets wants to be decapsulated,the mac address(src/dst) in the flow's match means the inner packets' mac address.Other match fields like dl_vlan is the vxlan packets' vlan.

eg:ovs-ofctl add-flow br0 in_port=4097,dl_vlan=1,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22,actions=2

3.The vxlan encapsulation flow do not support multiple ingress port(like lag,bond).Because vxlan encapsulation is in vcap,and vcap can not suport multiple ports.

4.Vxlan decapsulation flow's action also support group(type=all,lag-select-group),do not support modify mac or vlan before vxlan port 4097.

Command

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
```

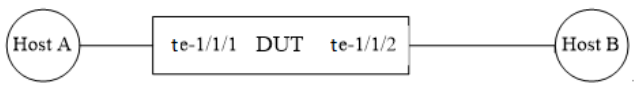
Description

1. br0: bridge name
2. remote_ip=10.10.10.2: the IP address of the peer VXLAN tunnel interface; this IP address will be the destination IP of the encapsulated VXLAN packets
3. local_ip=10.10.10.1: the IP address of this VXLAN tunnel interface; this IP address will be the source IP of the encapsulated VXLAN packets
4. src_mac==C8:0A:A9:9E:49:1A: the logical MAC address of the VXLAN tunnel interface; this MAC address will be the source MAC of the encapsulated VXLAN packets to next-hop
5. dst_mac=C8:0A:A9:9E:14:A5: the next-hop MAC address; this MAC address will be the destination MAC the encapsulated VXLAN packets to next-hop
6. egress_port=te-1/1/2: the output port of the encapsulated VXLAN packets
7. vnid=1234:the key value of VXLAN tunnel,different tunnel has different vnid.
8. vlan=1:the vlan of VXLAN tunnel.this vlan will be pop or not according to the pvid of the egress port.
9. udp_dst_port=4789:the udp destination port of encapsulating packets by VXLAN tunnel.All the encapsulated packets has the this udp dst port.

Examples

configure a VXLAN tunnel

topology



configuration

(1)create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

(2)add ports to br0.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

(3)add a VXLAN port named vxlan1 on te-1/1/2

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
```

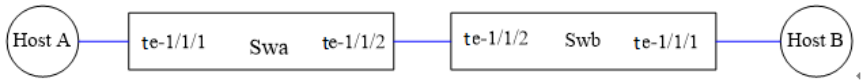
add a flow to switch

```
admin@PicOS-OVS$ovs-ofctl  add-flow br0 in_port=1,actions=output:4097
```

Send packets to te-1/1/1,te-1/1/2 will receive pakcets that encapsulated by VXLAN header. When VLAN of VXLAN tunnel is the same with the pvid of te-1/1/2,the packets from te-1/1/2 will be stripped VLAN of VXLAN. Or, packets will have two VLANs (outer VLAN is vxlan-vlan, inner VLAN is the pvid of ingress port or original VLAN of packets)

strip a VXLAN header

topology



configuration

User must configure VXLAN port on te-1/1/2 and te-1/1/3,and add some flows to the switches so that packets can be encapsulated or decapsulated and forwarded correctly.

(1) create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

(2) add ports to br0.

SwA:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

SWb:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

(3) add VXLAN port vxlan1 on egress port te-1/1/2 of switcha and switchb

Swa:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
```

flow in swa.

```
admin@PicOS-OVS$ovs-ofctl  add-flow br0 in_port=1,actions=output:4097
```

Swb:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.1
```

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=4097,actions= output:1
```

send packets to te-1/1/1 of swa,te-1/1/1 of switchb will receive the orignal packets(the contents of packets are the same with packets that te-1/1/1 of swa received).

configure two VXLAN tunnels on a pair of physical port

topology

configuration

add two pairs of VXLAN ports on te-1/1/2,te-1/1/3

sw1:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan2 -- set interface vxlan2 type=pica8_vxlan options:remote_ip=10.10.60.1
```

flows in sw1,

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:22:22:22:22:22,actions=output:4097
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:22:22:22:22:23,actions=output:4098
```

sw2:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.1
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan2 -- set interface vxlan2 type=pica8_vxlan options:remote_ip=10.10.60.1
```

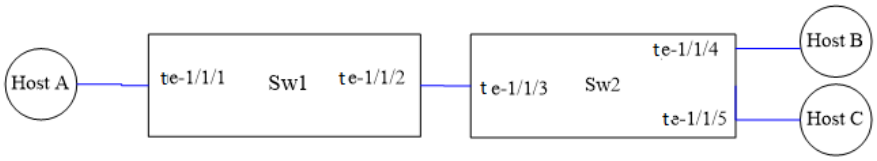
flows in sw2,

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=4097,dl_src=22:22:22:22:22:22,actions=output:4
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=4098,dl_src=22:22:22:22:22:23,actions=output:5
```

send packets to te-1/1/1 of sw1,te-1/1/4 should receive the packets with src_mac :22:22:22:22:22:22,and te-1/1/5 should receive the packets with src_mac 22:22:22:22:22:23.

collaboration between L2GRE and VXLAN

topology



configuration

User must configure VXLAN port and l2gre port on te-1/1/2 and te-1/1/3.Add flows on both switches, so packets can be forwarded correctly.

sw1:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
admin@PicOS-OVS$
ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.10 options:local_
```

flows in sw1,

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=output:4097
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:23,actions=output:5121
```

sw2:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.1
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set Interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.60.1
```

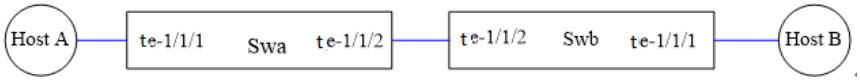
flows in sw2,

```
admin@PicOS-OVS$ovs-ofctl  add-flow br0 in_port=4097,dl_dst=22:22:22:22:22:22,actions=output:4
admin@PicOS-OVS$ovs-ofctl  add-flow br0 in_port=5121,dl_dst=22:22:22:22:22:23,actions=output:5
```

Vnid must be the same when the user wants to build a VXLAN tunnel between two ports. Different VXLAN tunnels must have different vnids. Besides, packets are not decapsulated when the vnid is different between the VXLAN tunnel. VXLAN can work together with GRE, L2GRE, VXLAN.

Option:

topology



Generally, untagged packets from Host A sent through Swa will be tagged by pvid in port te-1/1/1. The new tagged packet adds VXLAN header and strip VXLAN header through VXLAN tunnel, and will keep the tag while forwarding on Swb te-1/1/1 even though the tag equals the pvid of Swb te-1/1/1. The result is that Host B receives a tagged packet which is different from the original packet.

To avoid the above issue, pica8 support packet keep untag through pica8 switch port. The following command is necessary.

```
ovs-vsctl set interface te-1/1/1 options:access-vport=true
```

If the user adds the command on Swa, untagged packets that pass through Swa te-1/1/1 will not be tagged by the pvid, then pass through VXLAN tunnel and stay untagged while forwarding to Swb te-1/1/1. The result is Host B will receive untag packet.

vxlan numbers
User can create 1023 VXLAN ports at most (with the same mac, ip, vlan, only vnid is different) on one physical port. But the max flows number of VXLAN flow (with action=output:4097) is the minimum value of flows number that Vfilter table and Tcam table can support. That is 512 on P5401, P5101, AS6701, P5712,2632,tomahawk chip

Configure VxLAN Ecmp

From version 2.9.1, Pica8 switch support configuring Vxlan ecmp.That is to say,the traffic can hash to one or more ports of the ecmp.So the l3-ecmp-hash-fields is also valid to vxlan ecmp.And the egress port number suported is controlled by "ovs-vsctl set-max-ecmp-ports ",could be 2,4,8,16,32,default value is 4.

Command

```
ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2 options:local_
```

the usage is the same with vxlan.

.

Match Vxlan VNI

Introduction

From version 2.9.2, Pica8 switches support match vxlan vni fields.Platforms that supports VXLAN also supports matching VXLAN VNI field. The tun_id/tunnel_id uses the lower 24 bits in the lower 32 bits of the 64 bit vnid field.The higher 32 bits are 0x02000000. The udp, tp_dst and tun_id/tunnel_id are the necessary match fields, besides, you can match more fields like dl_vlan, dl_dst, dl_src, nw_src, nw_dst etc.The tp_dst must be the same with the configuration set by "*ovs-vsctl set-vxlan-udp-dst-port [port]*". This global configuration works well on vxlan decapsulation, but does not work on encapsualtion by vxlan tunnel.

Command

ovs-vsctl set-match-vxlan-vni-enable *[true/false]*: Please restart the Picos service after enabling or disabling the vxlan vni mode

ovs-vsctl set-vxlan-udp-dst-port *[port]*: Users can use this command to modify the layer 4 port number. The default value is 4789. If you want to recover the default value from another port number, use the command like this "*ovs-vsctl set-vxlan-udp-dst-port"*

Flow

ovs-ofctl add-flow br0 udp,tp_dst=5000,tun_id=0x0200000000112233,actions=2

> **flows info**
> 1.udp,tp_dst,tun_id are the necessary match fields, besides, you can match more fields like dl_vlan,dl_dst,dl_src,nw_src,nw_dst etc.
>
> 2.Actions could be set_field vlan vid, push_mpls etc. Vcap actions can not be supported(only push_vlan and only two pop_vlan etc)

Example1



step1: Configure bridge and port

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1 -- set interface te-1/1/1 type=pica8
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1 -- set interface te-1/1/2 type=pica8
ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1 -- set interface te-1/1/3 type=pica8
```

step2: Enable vxlan vni

```
ovs-vsctl set-match-vxlan-vni-enable true
```

step3:set ecmp select group and lag select group

```
ovs-vsctl set-group-ranges ecmp-select-groups=1-100,lag-select-groups=200-300
sudo systemctl restart picos
```

step4:add two groups

```
ovs-ofctl add-group br0 group_id=10,type=select,bucket=set_field:10-\>vlan_vid,set_field:00:00:00:22:22:22-\>dl_sr
ovs-ofctl add-group br0 group_id=200,type=select,bucket=set_field:1000-\>vlan_vid,set_field:00:00:00:11:11:11-\>et
```

step5:add a flow using ecmp-select-group

```
ovs-ofctl del-flows br0
ovs-ofctl add-flow br0 in_port=1,udp,tp_dst=4789,tun_id=0x0200000000112233,actions=group:10
```

step6:send src ip changing vxlan packets with tunnel id is 112233,udp dst port is 4789(vxlan dst mac is C8 0A A9 04 49 1A,vxlan src mac is C8 0A A9 9E 14 A5)

step7: add a flow using lag-select-group

```
ovs-ofctl del-flows br0
ovs-ofctl add-flow br0 in_port=1,udp,tp_dst=4789,tun_id=0x0200000000112233,dl_vlan=10,dl_dst=C8:0A:A9:04:49:1A,act
```

step8:send src ip changing vxlan packets with tunnel id is 112233,udp dst port is 4789(vxlan dst mac is C8 0A A9 04 49 1A,vxlan src mac is C8 0A A9 9E 14 A5)

Result

Step6:vxlan packets will hash to te-1/1/2,te-1/1/3.te-1/1/2 transmit the packets like this(dst mac is 00 00 00 33 33 33,src mac is 00 00 00 22 22 22 vlan is 10).te-1/1/3 transmit the packets like this (dst mac is 00 00 00 55 55 55,src mac is 00 00 00 44 44 44,vlan is 20)

Step8:vxlan packets will hash to te-1/1/2,te-1/1/3.te-1/1/2 and te-1/1/3 transmit the same vxlan packets like this(dst mac is 00 00 00 11 11 11,src mac is C8 0A A9 9E 14 A5,vlan is 1000)

Multiple vxlan output port

From 4.1.0, ovs support multiple vxlan output port in flow, such as “in_port=1,actions=output:4097,output:4098”. You must use this command “ovs-vsctl set-port-default-flood true” to use this function.

Note:the multiple vxlan tunnels’ vnid must the same, but the egress ports can be different or the same, both are ok.

Example

step1,enable default flood and restart picos service first.

```
admin@PICOS-OVS:~$ ovs-vsctl set-port-default-flood true
 Please reboot for the change to take effect!
admin@PICOS-OVS:~$ sudo /etc/init.d/picos restart
```

step2,create two vxlan tunnels

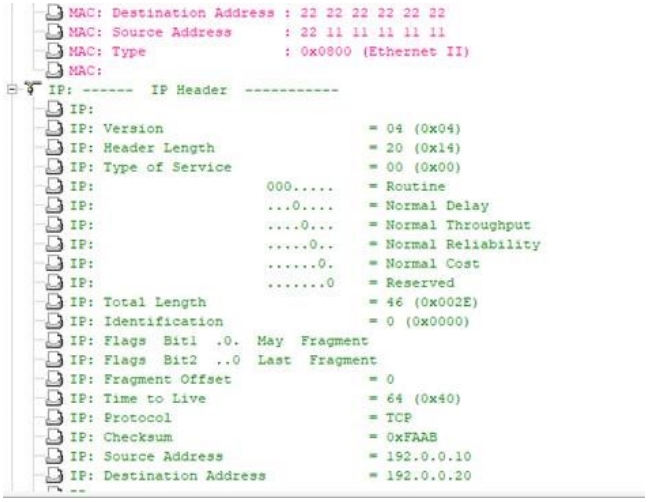
```
admin@PICOS-OVS:~$ ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.1

admin@PICOS-OVS:~$ ovs-vsctl add-port br0 vxlan2 -- set interface vxlan2 type=pica8_vxlan options:remote_ip=20.20.1
```

step3,add flow

```
admin@PICOS-OVS:~$ ovs-ofctl add-flow br0 in_port=17,actions=output:4097,output:4098

admin@PICOS-OVS:~$ ovs-ofctl add-flow br0 in_port=4097,actions=17

admin@PICOS-OVS:~$ ovs-ofctl add-flow br0 in_port=4098,actions=17
```

step4,send packets to port 17,then check the vxlan packets of port 18,port 18 should transmit two kinds of vxlan ports.

te-1/1/17 receive packets:



Te-1/1/18:One kind is like this:

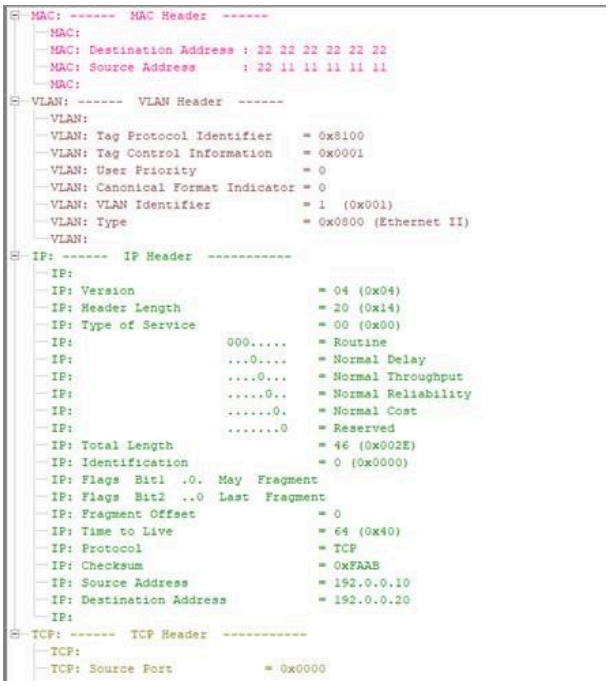
```
MAC: ------  MAC Header  ------
    MAC:
    MAC: Destination Address : C8 0A A9 9E 14 A5
    MAC: Source Address      : C8 0A A9 04 49 1A
    MAC: Type                : 0x0800 (Ethernet II)
    MAC:
IP: ------  IP Header  ----------
    IP:
    IP: Version                         = 04 (0x04)
    IP: Header Length                   = 20 (0x14)
    IP: Type of Service                 = 00 (0x00)
    IP:                   000.....      = Routine
    IP:                   ...0....      = Normal Delay
    IP:                   ....0...      = Normal Throughput
    IP:                   .....0..      = Normal Reliability
    IP:                   ......0.      = Normal Cost
    IP:                   .......0      = Reserved
    IP: Total Length                    = 100 (0x0064)
    IP: Identification                  = 43589 (0xAA45)
    IP: Flags  Bit1  .0.  May  Fragment
    IP: Flags  Bit2  ..0  Last  Fragment
    IP: Fragment Offset                 = 0
    IP: Time to Live                    = 64 (0x40)
    IP: Protocol                        = UDP
    IP: Checksum                        = 0xA82D
    IP: Source Address                  = 10.10.10.1
    IP: Destination Address             = 10.10.10.2
    IP:
UDP: ------  UDP Header  ----------
    UDP:
    UDP: Source Port         = 5555 (0x15B3)
    UDP: Destination Port    = 4789 (0x12B5)
    UDP: Length              = 80 (0x0050)
    UDP: Checksum            = 0 (0x0000)
    UDP:
```

Te-1/1/18:the other kind like this:

```
MAC: ------  MAC Header  ------
    MAC:
    MAC: Destination Address : 88 88 88 88 88 88
    MAC: Source Address      : 66 66 66 66 66 66
    MAC:
VLAN: ------  VLAN Header  ------
    VLAN:
    VLAN: Tag Protocol Identifier    = 0x8100
    VLAN: Tag Control Information    = 0x000A
    VLAN: User Priority              = 0
    VLAN: Canonical Format Indicator = 0
    VLAN: VLAN Identifier            = 10  (0x00A)
    VLAN: Type                       = 0x0800 (Ethernet II)
    VLAN:
IP: ------  IP Header  ----------
    IP:
    IP: Version                         = 04 (0x04)
    IP: Header Length                   = 20 (0x14)
    IP: Type of Service                 = 00 (0x00)
    IP:                   000.....      = Routine
    IP:                   ...0....      = Normal Delay
    IP:                   ....0...      = Normal Throughput
    IP:                   .....0..      = Normal Reliability
    IP:                   ......0.      = Normal Cost
    IP:                   .......0      = Reserved
    IP: Total Length                    = 100 (0x0064)
    IP: Identification                  = 24005 (0x5DC5)
    IP: Flags  Bit1  .0.  May  Fragment
    IP: Flags  Bit2  ..0  Last  Fragment
    IP: Fragment Offset                 = 0
    IP: Time to Live                    = 64 (0x40)
    IP: Protocol                        = UDP
    IP: Checksum                        = 0xCC99
    IP: Source Address                  = 20.20.20.1
    IP: Destination Address             = 20.20.20.2
    IP:
UDP: ------  UDP Header  ----------
    UDP:
    UDP: Source Port         = 5555 (0x15B3)
    UDP: Destination Port    = 4789 (0x12B5)
    UDP: Length              = 80 (0x0050)
```

step5,Send above two kinds of vxlan packets to te-1/1/18,then te-1/1/17 will transmit the decapsulated packets.

te-1/1/17 transmit packets like this:


MAC: ------ MAC Header ------
MAC:
MAC: Destination Address : 22 22 22 22 22 22
MAC: Source Address : 22 11 11 11 11 11
MAC:
VLAN: ------ VLAN Header ------
VLAN:
VLAN: Tag Protocol Identifier = 0x8100
VLAN: Tag Control Information = 0x0001
VLAN: User Priority = 0
VLAN: Canonical Format Indicator = 0
VLAN: VLAN Identifier = 1 (0x001)
VLAN: Type = 0x0800 (Ethernet II)
VLAN:
IP: ------ IP Header ----------
IP:
IP: Version = 04 (0x04)
IP: Header Length = 20 (0x14)
IP: Type of Service = 00 (0x00)
IP: 000..... = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: ......0. = Normal Cost
IP: ....0 = Reserved
IP: Total Length = 46 (0x002E)
IP: Identification = 0 (0x0000)
IP: Flags Bit1 .0. May Fragment
IP: Flags Bit2 ..0 Last Fragment
IP: Fragment Offset = 0
IP: Time to Live = 64 (0x40)
IP: Protocol = TCP
IP: Checksum = 0xFAAB
IP: Source Address = 192.0.0.10
IP: Destination Address = 192.0.0.20
IP:
TCP: ------ TCP Header ----------
TCP:
TCP: Source Port = 0x0000

Decapsulation by pop actions

From version 3.2,pica8 switch support another decapsulation way.Users can use pop_vxlan/pop_l2gre/pop_gre to decapsulate the vxlan/l2gre/gre packets.If you want to use this kind of decapsulation way,you should enable npb mode first by command **"ovs-vsctl enable-npb-mode true".**Then need to retart the picos serviece(sudo /etc/init.d/picos restart).After the restarting,you can use this way to do some decapsulation.

Notes
1.The tunnels created on different ports/same ports must have different source ips to ensure that these tunnels can be decapsulated normally. If the ips in these tunnels are the same,then some problems will occur.
2.Multiple tunnels are created on the same port. The src mac, dst mac, and vlan of these tunnels must be the same to ensure that these tunnel encapsulations work properly. Decapsulation is not subject to this limitation.
3.Pop_gre to work with pop_l2gre and pop_vxlan at the same time, you must ensure that pop_gre flow has a lower priority than pop_l2gre|pop_vxlan.
4.The location of pop_vxlan/pop_l2gre in the flow action has no relationship and can be decapsulated normally.

5.do not match tunnel_id feature only supported on 5812.

POP_Vxlan

There are two ways including matching tunnel_id or do not match tunnel_id.The matching fields must include **"in_port,dl_dst,ip,nw_src,nw_dst,tunnel_id"** or **"in_port,dl_dst,nw_src,nw_dst,udp,tp_dst=4789".**

```
admin@PICOS-OVS:~$ ovs-ofctl add-flow br0 in_port=2,dl_dst=c4:39:3a:fb:be:d9,ip,nw_src=10.10.2.20,nw_dst=10.10.1.2(
```

```
admin@PICOS-OVS:~$ ovs-ofctl add-flow br0 in_port=6,dl_dst=44:44:44:44:44:44,nw_src=255.255.255.100,nw_dst=255.255
```

Pop_l2gre

There are two ways including matching tunnel_id or do not match tunnel_id.The matching fields must include **"in_port,dl_dst,ip,nw_src,nw_dst,tunnel_id"** or **"in_port,dl_dst,nw_src,nw_dst".**

```
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 in_port=2,dl_dst=c4:39:3a:fb:be:d9,ip,nw_src=10.10.60.10,nw_dst=10.10.61.1
```

```
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 in_port=6,dl_dst=66:66:66:66:66:66,ip,nw_src=20.20.20.20,nw_dst=40.40.40.4
```

Pop_gre

```
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 in_port=2,ip,dl_vlan=1000,dl_dst=C8:0A:A9:9E:14:A5,nw_src=10.10.60.10,nw_(
```

Configuring Bridge and Ports

Configuring bridge

Users can create one or more bridges on a PICA8 switch. Note that each physical port can only be added to one bridge.

User can use command 'ovs-appctl pica/show' to show valid ports.

```
admin@PicOS-OVS$ovs-appctl pica/show
Max Hardware Flow Entry Limitation:
    TCAM Table    : 2048
    Egress Table  : 256
    VFilter Table : 1024
    L2 Table      : 32768
    L3 Table      : 24000
Valid Interfaces On Switch P3290:
    Physical interfaces:
        ge-1/1/1(1)       ge-1/1/2(2)       ge-1/1/3(3)       ge-1/1/4(4)
        ge-1/1/5(5)       ge-1/1/6(6)       ge-1/1/7(7)       ge-1/1/8(8)
        ge-1/1/9(9)       ge-1/1/10(10)     ge-1/1/11(11)     ge-1/1/12(12)
        ge-1/1/13(13)     ge-1/1/14(14)     ge-1/1/15(15)     ge-1/1/16(16)
        ge-1/1/17(17)     ge-1/1/18(18)     ge-1/1/19(19)     ge-1/1/20(20)
        ge-1/1/21(21)     ge-1/1/22(22)     ge-1/1/23(23)     ge-1/1/24(24)
        ge-1/1/25(25)     ge-1/1/26(26)     ge-1/1/27(27)     ge-1/1/28(28)
        ge-1/1/29(29)     ge-1/1/30(30)     ge-1/1/31(31)     ge-1/1/32(32)
        ge-1/1/33(33)     ge-1/1/34(34)     ge-1/1/35(35)     ge-1/1/36(36)
        ge-1/1/37(37)     ge-1/1/38(38)     ge-1/1/39(39)     ge-1/1/40(40)
        ge-1/1/41(41)     ge-1/1/42(42)     ge-1/1/43(43)     ge-1/1/44(44)
        ge-1/1/45(45)     ge-1/1/46(46)     ge-1/1/47(47)     ge-1/1/48(48)
        te-1/1/49(49)     te-1/1/50(50)     te-1/1/51(51)     te-1/1/52(52)
    LAG   interfaces:    ae1(1025) - ae1023(2047)
    Bond  interfaces:  bond1(2049) - bond1023(3071)
    GRE   interfaces:   gre1(3073) - gre1023(4095)
    VXLAN interfaces: vxlan1(4097) - vxlan1023(5119)
    L2GRE interfaces: l2gre1(5121) - l2gre1023(6143)
```

Create a Bridge

User can command "**ovs-vsctl add-br *<bridge> [-- set bridge br0 datapath_type=pica8]***".

From PicOS2.6.5, due to the default datapath_type is pica8, so "***-- set bridge br0 datapath_type=pica8***" is optional.

```
root@PicOS-OV$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
root@PicOS-OVS$ovs-vsctl add-br br1
```

Viewing the Bridge Settings

Use the **show <bridge_name>** command to view the bridge details.

```
root@PicOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (xid=0x1): ver:0x1, dpid:0000e89a8f503d30
n_tables:1, n_buffers:256
features: capabilities:0x87, actions:0x3f
1(ge-1/1/1): addr:e8:9a:8f:50:3d:30
config: 0
state: LINK_DOWN
current: 10MB-FD COPPER AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
advertised: 10MB-FD AUTO_PAUSE
supported: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
peer: 10MB-FD AUTO_PAUSE
2(ge-1/1/2): addr:e8:9a:8f:50:3d:30
config: 0
state: LINK_DOWN
current: 10MB-FD COPPER AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
advertised: 10MB-FD AUTO_PAUSE
supported: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
```

```
peer: 10MB-FD AUTO_PAUSE
3(ge-1/1/3): addr:e8:9a:8f:50:3d:30
config: 0
state: LINK_DOWN
current: 10MB-FD COPPER AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
advertised: 10MB-FD AUTO_PAUSE
supported: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD AUTO_NEG AUTO_PAUSE AUTO_PAUSE_ASYM
peer: 10MB-FD AUTO_PAUSE
LOCAL(br0): addr:e8:9a:8f:50:3d:30
config: PORT_DOWN
state: LINK_DOWN
current: 10MB-FD COPPER
OFPT_GET_CONFIG_REPLY (xid=0x3): frags=normal miss_send_len=0
root@PicOS-OVS$
root@PicOS-OVS$
root@PicOS-OVS$ ovs-vsctl list-ports br0
ge-1/1/1
ge-1/1/2
ge-1/1/3
root@PicOS-OVS$
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list-ifaces br0
ge-1/1/1
ge-1/1/2
ge-1/1/3
root@PicOS-OVS$
root@PicOS-OVS$
```

Deleting the Bridge

To delete the bridge and its ports, use the **del-port** command, then the **del-br <bridge_name>** command.

```
root@PicOS-OVS$ovs-vsctl  del-port br0 ge-1/1/1
root@PicOS-OVS$ovs-vsctl  del-port br0 ge-1/1/2
root@PicOS-OVS$ovs-vsctl  del-port br0 ge-1/1/3
root@PicOS-OVS$ovs-vsctl  del-br br0
```

View software table flows

Normally,we view software table flows using below command without options.

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
```

And picos add a cli view to group flows into certain application categories (LLDP, VRRP, IP, Controller, Miscellaneous) or a user-configurable value from Picos 2.8.0. User can filter flows using the flow group name.

ovs-ofctl dump-flows br0 --filter=<VRRP | LLDP | IPV4 | IPV6 | CONTROLLER | MISC>

You can use one filter or more.

For example:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0 --filter=VRRP,LLDP,IPV4,IPV6,CONTROLLER,MISC

VRRP flows (count=1):
 flow_id=9, cookie=0x0, duration=64.268s, table=0, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=1,dl_dst=01

LLDP flows (count=1):
 flow_id=6, cookie=0x0, duration=92.408s, table=0, n_packets=n/a, n_bytes=0, in_port=3,dl_dst=01:80:c2:00:00:0e,dl_

IPV4 flows (count=2):
 flow_id=9, cookie=0x0, duration=64.268s, table=0, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=1,dl_dst=01
 flow_id=8, cookie=0x0, duration=72.908s, table=0, n_packets=n/a, n_bytes=0, ip,in_port=2,nw_dst=192.168.100.200 a

IPV6 flows (count=1):
 flow_id=10, cookie=0x0, duration=57.592s, table=0, n_packets=n/a, n_bytes=0, tcp6,in_port=3 actions=CONTROLLER:65

Controller flows (count=2):
 flow_id=8, cookie=0x0, duration=72.908s, table=0, n_packets=n/a, n_bytes=0, ip,in_port=2,nw_dst=192.168.100.200 a
 flow_id=10, cookie=0x0, duration=57.592s, table=0, n_packets=n/a, n_bytes=0, tcp6,in_port=3 actions=CONTROLLER:65
```

```
MISC flows (count=1):
 flow_id=7, cookie=0x0, duration=80.295s, table=0, n_packets=n/a, n_bytes=0, priority=40000,in_port=3,dl_dst=01:80
admin@PicOS-OVS$
```

Enable STP in bridge

Defaultly, STP is disabled in ovs mode. User can use following command to enable/disable STP in bridge.

ovs-vsctl set bridge <*bridge*> stp_enable=<*true*|*false*>

Example:

```
admin@PicOS-OVS$ovs-vsctl set bridge br-12 stp_enable=true

admin@PicOS-OVS$ovs-ofctl show br-12
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2):
dpid:0xaa5e60eb69d29cd7(12276356198467542231)
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
 51(te-1/1/51): addr:60:eb:69:d2:9c:d7
     config:     0
     state:      BLOCKED
     current:    10GB-FD FIBER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 10000 Mbps now, 10000 Mbps max
 52(te-1/1/52): addr:60:eb:69:d2:9c:d7
     config:     0
     state:      LINK_UP
     current:    10GB-FD FIBER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 10000 Mbps now, 10000 Mbps max
 LOCAL(br-12): addr:60:eb:69:d2:9c:d7
     config:     0
     state:      LINK_UP
     current:    10MB-FD COPPER
     supported:  10MB-FD COPPER
     speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.4) (xid=0x5): frags=normal miss_send_len=0
```

Other_config about bridge

1)Configure datapath-id:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:datapath-id=0000d80aa99e14a3
```

2)Human readable description of datapath:

```
admin@PicOS-OVS$ovs-vsctl set bridg br0 other_config:dp-desc=pica8
```

3)Disable or enable in-band:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other-config:disable-in-band=true/false
```

4)The flow table will be cleared or not:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:enable-flush=true/false
```

5)This sets the OpenFlow queue ID that will be used by flows set up by in-band control on this bridge:

```
admin@PicOS-OVS$ovs-vsctl set bridg br0 other_config:in-band-queue=4
```

Note: in-band-queue is in range 0 to 7.

6)Configure stp:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:stp-priority=0x7800
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:stp-system-id=123456
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:stp-hello-time=10
```

Note：stp hello time is in range 1 to 10.

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:stp-max-age=6
```

Note：stp max age is in range 6 to 40.

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:stp-forward-delay=6
```

Note：stp-forward-delay **is in range 4 to 30.**

7)Specifies the number of threads for software datapaths to use for handling new flows:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:n-handler-threads=1
```

8)Specifies the number of threads for software datapaths to use for revalidating flows in the Datapath:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:n-revalidator-threads=2
```

9)The maximum number of seconds to retain a MAC learning entry for which no packets have been seen.

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:mac-aging-time=300
```

10)The maximum number of MAC addresses to learn.

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:mac-table-size=2048
```

11)LLDP:

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-msg-tx-hold=4
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-msg-tx-interval=30
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-reinit-delay=2
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tx-delay=2
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-port-desc=false
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-name=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-desc=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-sys-cap=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mgmt-addr=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-pvid=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-mac-phy=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-power-via-mdi=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-max-frame-size=true
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:lldp-tlv-link-aggregation=true
```

12)Configure bridge mac address.

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 other_config:hwaddr=22:22:22:22:22:22
```

Configuring CDR

Clock and Data Recovery (CDR) is a process that is dependent upon a clock signal synchronous with the data flow. When a data flow arrives at the receiver, it is sent without additional clocking information, the receiver generates a clock from an approximate frequency reference, and then phase-aligns the clock to the transitions in the data flow with a phase-locked loop (PLL). Data distortion, noise, and jitter on the incoming data can be reduced if the CDR technology is used for data recovery from the transmission channel.

NOTEs:

- CDR function can only be configured on the 800G, 400G, 200G, 100G or 40G optical module interface and the split interfaces broke out from them.
- The CDR configurations of split interfaces which broke out from the 800G, 400G, 200G, 100G or 40G optical module interface should be the same.

Procedure

- Use the following command to disable or enable the CDR function.

  ovs-vsctl set interface <*interface-name*> options:cdr-admin-state=[true | false]

  The default setting is **true**. The command takes effect immediately after committing.

- Use the following command to remove CDR function.

  ovs-vsctl remove interface <*interface-name*> options cdr-admin-state

Configuration Example

- Enable the CDR function on interface te-1/1/1~te-1/1/4.

```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/1 options:cdr-admin-state=true
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/2 options:cdr-admin-state=true
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/3 options:cdr-admin-state=true
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/4 options:cdr-admin-state=true
```

- Disable the CDR function on interface te-1/1/1~te-1/1/4.

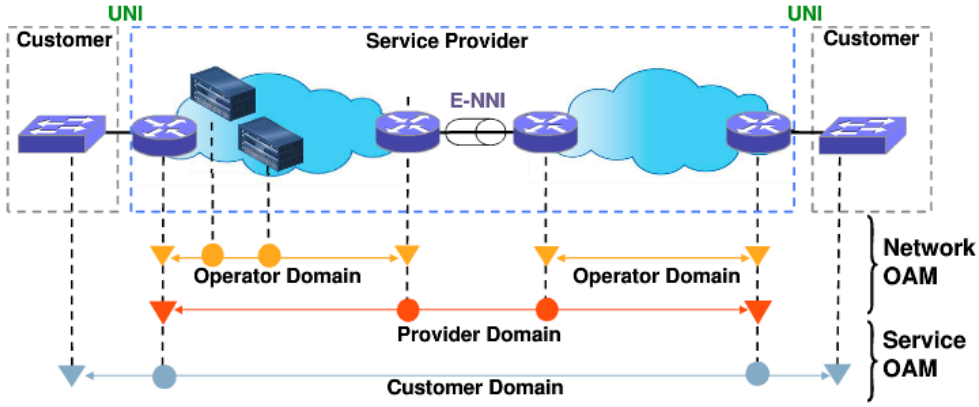
```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/1 options:cdr-admin-state=false
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/2 options:cdr-admin-state=false
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/3 options:cdr-admin-state=false
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/4 options:cdr-admin-state=false
```

- Remove the CDR function on interface te-1/1/1~te-1/1/4.

```
admin@PICOS-OVS$ovs-vsctl remove interface te-1/1/1 optionscdr-admin-state
admin@PICOS-OVS$ovs-vsctl remove interface te-1/1/2 optionscdr-admin-state
admin@PICOS-OVS$ovs-vsctl remove interface te-1/1/3 optionscdr-admin-state
admin@PICOS-OVS$ovs-vsctl remove interface te-1/1/4 optionscdr-admin-state
```

Configuring CFM

Connectivity Fault Management (CFM) is an IEEE standard, 802.1ag, which specifies protocols, procedures, and managed objects to support transport fault management. CFM is used for detecting link connectivity fault, confirming the fault and locating the fault in the network.



The standard, 802.1ag defines:

- Maintenance domains (MD), their constituent maintenance points (MIP, MEP), and the managed objects (MA) required to create and administer them.
- The relationship between maintenance domains and the services offered by VLAN-aware bridges and provider bridges.
- The description of protocols and procedures used by maintenance points to maintain and diagnose connectivity faults within a maintenance domain.
- Means for future expansion of the capabilities of maintenance points and their protocols.

As illustrated in the above figure, each domain (operator, provider, customer) is allocated. Maintenance association Intermediate endPoint (MIP) and Maintenance domain End Point (MEP) essentially define the domain boundaries and the intermediate elements. Effectively, these end-points define a fault-domain which aids in building a flexible fault-management framework. Network and Service OAM shown above, are typically used to represent faults to a network operator and a service consumer.

IEEE 802.1ag Ethernet CFM (Connectivity Fault Management) protocols comprise three protocols that work together to help administrators debug Ethernet networks. They are:

Continuity Check Protocol (CCP) - Heartbeat messages for CFM. The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. CCMs are multicast messages. CCMs are confined to a domain (MD). These messages are unidirectional and do not solicit a response. Each MEP transmits a periodic multicast Continuity Check Message inward towards the other MEPs.

Link Trace (LT) - Link Trace messages otherwise known as Mac Trace Route, are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP, which is similar in concept to User Datagram Protocol(UDP) Trace Route. Each receiving MEP sends a Trace Route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

Loop-back (LB) - Loop-back messages otherwise known as MAC ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loopback to successive MIP's can determine the location of a fault. Sending a high volume of Loopback Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. An MEP can send a Loopback to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

Monitor connectivity to a remote maintenance point on ge-1/1/1

Set the MPID of CFM:

```
admin@PicOS-OVS$ ovs-vsctl set Interface ge-1/1/1 cfm_mpid=2333
```

A Maintenance Point ID (MPID) uniquely identifies each endpoint within a Maintenance Association. According to the 802.1ag specification, MPIDs can only range between [1, 8191].

Set extended mode:

```
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_extended=true
```

Extended mode increases the accuracy of the cfm_interval configuration parameter by breaking wire compatibility with 802.1ag compliant implementations. An extended mode allows **eight byte MPIDs**.

Set demand mode:

```
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_demand=true
```

When true, and cfm_extended is true, the CFM module operates in demand mode. By default it is set to false. When in demand mode, traffic received on the Interface is used to indicate liveness. CCMs are still transmitted and received. At least one CCM must be received every 100 * cfm_interval amount of time. Otherwise, even if traffic is received, the CFM module will trigger the connectivity fault. Demand mode disables itself when there are multiple remote maintenance points.

Set the requested transmission interval:

```
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_interval=10000
```

In standard mode supports intervals of 3, 10, 100, 1000, 10000,60000, or 600000 ms are supported. Extended mode supports any interval up to 65535 ms and default is 1000 ms. However, we do not recommend intervals less than 100 ms.

Set CCM VLAN tag:

```
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_ccm_vlan=2000
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_ccm_vlan=random
```

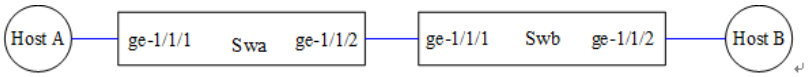
When set, the CFM module will apply a VLAN tag to all CCMs it generates with the given value.

Set CCM Priority:

```
admin@PicOS-OVS$ovs-vsctl set Interface ge-1/1/1 other_config:cfm_ccm_pcp=7
```

When set, the CFM module will apply a VLAN tag to all CCM's, it generates with the given PCP value, the VLAN ID of the tag is governed by the value of "cfm_ccm_vlan". If "cfm_ccm_vlan" is unset, a VLAN ID of zero is used.

CFM Example



Step 1: Basic configuration

DUT1:

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1  -- set Interface ge-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1  -- set Interface ge-1/1/2 type=pica8
```

DUT2:

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1  -- set Interface ge-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1  -- set Interface ge-1/1/2 type=pica8
```

Step 2: Configure cfm:

DUT1:

```
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/2 cfm-mpid=8999
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/2 other_config:cfm_extended=true
```

DUT2:

```
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 cfm-mpid=9000
admin@PicOS-OVS$ovs-vsctl set interface ge-1/1/1 other_config:cfm_extended=true
```

Step 3: Check packets

DUT1:

Check list interface:

```
admin@PicOS-OVS$ovs-vsctl list interface ge-1/1/2
_uuid : 94942d57-d9a8-4030-ad3b-483dadbd7926
admin_state : up
bfd : {}
bfd_status : {}
cfm_fault : false
cfm_fault_status : []
```

```
cfm_flap_count : 2
cfm_health : []
cfm_mpid : 8999
cfm_remote_mpids : [9000]
cfm_remote_opstate : up
duplex : full
external_ids : {}
ifindex : 13
ingress_policing_burst: 0
ingress_policing_rate: 0
lacp_current : []
link_resets : 0
link_speed : 1000000000
link_state : up
mac : []
mac_in_use : "00:e0:ec:25:2d:5e"
mtu : 9212
name : "ge-1/1/2"
ofport : 13
ofport_request : []
options : {}
other_config : {cfm_extended="true"}
statistics : {collisions=0, rx_bytes=3255, rx_crc_err=0, rx_dropped=28, rx_errors=0, rx_frame_err=0, rx_over_err=0
status : {}
type : "pica8"
wred_queues : {}
```

Check cfm/show:

```
admin@PicOS-OVS$ovs-appctl  cfm/show
---- ge-1/1/2 ----
MPID 8999: extended
                average health: undefined
                opstate: up
                remote_opstate: up
                interval: 1000ms
                next CCM tx: 481ms
                next fault check: 973ms
Remote MPID 9000
                recv since check: true
                opstate: up
admin@PicOS-OVS$
```

Check hardware table:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#168 normal permanent priority=18000000,in_port=2,dl_dst=01:23:20:00:00:30,dl_type=0x8902, actions:userspace(pid=0
#167 normal permanent priority=0, actions:drop
Total 2 flows in HW.
```

DUT2:

Check list interface:

```
admin@PicOS-OVS$ovs-vsctl list interface ge-1/1/1
_uuid : 61bb8ef5-30f9-4855-8cfa-f1ee0bc5b154
admin_state : up
bfd : {}
bfd_status : {}
cfm_fault : false
cfm_fault_status : []
cfm_flap_count : 0
cfm_health : []
cfm_mpid : 9000
cfm_remote_mpids : [8999]
cfm_remote_opstate : up
duplex : full
external_ids : {}
ifindex : 11
ingress_policing_burst: 0
```

```
ingress_policing_rate: 0
lacp_current : []
link_resets : 0
link_speed : 1000000000
link_state : up
mac : []
mac_in_use : "08:9e:01:a8:00:49"
mtu : 9212
name : "ge-1/1/11"
ofport : 11
ofport_request : []
options : {}
other_config : {cfm_extended="true"}
statistics : {collisions=0, rx_bytes=1302, rx_crc_err=0, rx_dropped=8, rx_errors=0, rx_frame_err=0, rx_over_err=0,
status : {}
type : "pica8"
wred_queues : {}
admin@PicOS-OVS$
```

Check cfm/show:

```
admin@PicOS-OVS$ovs-appctl  cfm/show
---- ge-1/1/1 ----
MPID 9000: extended
                average health: undefined
                opstate: up
                remote_opstate: up
                interval : 1000ms
                next CCM tx: 802ms
                next fault check: 1254ms
Remote MPID 8999
                recv since check: true
                opstate: up
admin@PicOS-OVS$
```

Check hardware table:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#168 normal permanent priority=18000000,in_port=1,dl_dst=01:23:20:00:00:30,dl_type=0x8902, actions:userspace(pid=0
#167 normal permanent priority=0, actions:drop
Total 2 flows in HW.
```

> Standard mode, dl_mac is 01:80:c2:00:00:30; when extended mode,the dst mac is 01:23:20:00:00:30.

Configue cfm on port ge-1/1/13, if delete cfm

```
admin@PicOS-OVS$ovs-vsctl clear interface ge-1/1/13 cfm_mpid
admin@PicOS-OVS$ovs-vsctl remove interface ge-1/1/13 other_config cfm_interval="10000"
admin@PicOS-OVS$ovs-vsctl remove interface ge-1/1/13 other_config cfm_extended="true"
admin@PicOS-OVS$ovs-vsctl remove interface ge-1/1/13 other_config cfm_ccm_vlan=random
```

Configuring LFS

Abstract

Link fault signaling operates between the remote RS and the local RS. Faults detected between the remote RS and the local RS are received by the local RS as Local Fault. Only an RS originates Remote Fault signals.

Sub-layers within the PHY are capable of detecting faults that render a link unreliable for communication. Upon recognition of a fault condition, a PHY sub-layer indicates Local Fault status on the data path. When this Local Fault status reaches an RS, the RS stops sending MAC data, and continuously generates a Remote Fault status on the transmit data path (possibly truncating a MAC frame being transmitted). When Remote Fault status is received by an RS, the RS stops sending MAC data, and continuously generates Idle control characters. When the RS no longer receives fault status messages, it returns to normal operation, sending MAC data.

The RS reports the fault status of the link. Local Fault indicates a fault detected on the receive data path between the remote RS and the local RS. Remote Fault indicates a fault on the transmit path between the local RS and the remote RS.

The fault status is as follows:

a) link_fault = OK

The RS shall send MAC frames as requested through the PLS service interface. In the absence of MAC frames, the RS shall generate Idle control characters.

b) link_fault = Local Fault

The RS shall continuously generate Remote Fault Sequence ordered_sets.

c) link_fault = Remote Fault

The RS shall continuously generate Idle control characters.

Link Fault Signaling

If ignore local fault is set as false. When link local fault is triggered, the RS shall continuously generate Remote Fault Sequence ordered_sets. Otherwise, the RS will not generate Remote Fault Sequence ordered_sets.

If ignore remote fault is set as false. When link remote fault is received, The RS shall continuously generate Idle control characters. Other, The RS shall send MAC frames as requested through the PLS service interface and generate Idle control characters in the absence of MAC frames.

LFS Commands

The following is the configuration command as sample:

```
ovs-vsctl set Interface te-1/1/1 options:link-fault-signaling=ignore-none
ovs-vsctl set Interface te-1/1/1 options:link-fault-signaling=ignore-local
ovs-vsctl set Interface te-1/1/1 options:link-fault-signaling=ignore-remote
ovs-vsctl set Interface te-1/1/1 options:link-fault-signaling=ignore-both
```

1. "ignore-local" means ignoring local signaling fault.
2. "ignore-remote" means ignoring local remote fault.
3. "ignore-both" means ignoring both local and remote signaling fault.
4. "ignore-none" means not ignoring neither local signaling fault nor remote signaling fault.

Up Mode

The force up command forcibly brings up a fiber Ethernet port and enables the port to forward packets uni-directionally over a single link. In this way, transmission links are well utilized.

Up mode commands.

The following is the configuration command as a sample:

```
ovs-vsctl set Interface te-1/1/1 options:up-mode=true
ovs-vsctl set Interface te-1/1/1 options:up-mode=false
```

1. Disable port command has a higher priority than set port up command. If one port is disabled manually, it is not effective to set it up forcibly.

2. Up-mode true command should be configured together with ignore-local-fault true command. If user only configures up-mode true and not ignore-local-fault command, traffic can't transmit from TX link

3. LFS command must configurate on more than 10G port.

Configuring Loopback

Loop the traffic which into switch back to ingress.

It is possible to configure the egress interface to be the ingress interface.

PicOS supports loopback interface in hardware. By default, a packet coming into an interface cannot be sent back to the same interface via Openflow. That means the user cannot configure a flow whose output port is the "in_port". For example, the following flow will not work in hardware by default:

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=in_port
```

This behavior can be changed with the following commands:

```
ovs-appctl loopback/enable true
```

This is supported starting in PicOS 2.2. It should only be used for specific traffic as it can be dangerous to send broadcast traffic back on the same port on a Layer 2 network.

Except this one, also supports another command to enable loopback. This one will replace above command.

```
root@PicOS-OVS#ovs-vsctl set-loopback-enable true
```

With the above configuration, hardware can allow the flow output port to be the same as in_port. The user can disable the loopback interface with the following command:

```
ovs-vsctl set-loopback-enable false
```

Users should know the limitation of the loopback interface in hardware. In the OpenFlow Specification, there are some actions (Flood, Group table, for example) that are for broadcasting. The packet should not be forwarded back to the **in_port** port. Be cautious using the enable loopback interface, so that the packet is not forwarded back to the in_port port.

Example1, loop the traffic back to in_port.

```
admin@PicOS-OVS$ovs-vsctl set-loopback-enable true
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=in_port
```

Example2, loop the traffic back to in_port and same time send out from others.

```
admin@PicOS-OVS$ovs-vsctl set-loopback-enable true
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=in_port,all
```

⚠ 1, The port can be physical port, lag interface.

Loop the traffic which out from switch back to switch again.

From version 2.8.1, PicOS also support enable loop in interface, and the feature is different from above.

User can configure one or more ports as loopbcak port. Thus, traffic can be outputed and loopback to itself. The port can be plugin module or not.

Command:

ovs-vsctl set interface <port> options:loopback=true|false

<port>: ***can be physical port, lag port and GRE/L2GRE/VxLAN tunnel port.***

Configure port te-1/1/1 as a loopback port:

```
ovs-vsctl set interface te-1/1/1 options:loopback=true
```

Example1, Modify traffic dl_dst=22:22:22:11:11:11 and out from port14, then modify dl_dst=22:22:22:22:22:22 and out from port25.

Need configure two port as loopback port, use port2 and port3 here.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:loopback=true
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/3 options:loopback=true
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:2,3
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=2,actions=set_field:22:22:22:11:11:11-\>eth_dst,output:14
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=3,actions=set_field:22:22:22:22:22:22-\>eth_dst,output:25
```

Example2, traffic after encap vxlan then go through L3 flow table.

Configure loopback in physical port.

```
admin@PicOS-OVS$ovs-vsctl set-l2-mode true
admin@PicOS-OVS$ovs-vsctl set-l3-mode true
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:loopback=true
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=output:4097
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=251,dl_vlan=1,dl_dst=C8:0A:A9:9E:14:A5,actions=normal
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=252,ip,nw_dst=10.10.10.2,actions=set_field:100-\>vlan_vid,set_field:2
```

Example2, traffic go through L3 flow table then discap vxlan.

Configure loopback in physical port.

```
admin@PicOS-OVS$ovs-vsctl set-l2-mode true
admin@PicOS-OVS$ovs-vsctl set-l3-mode true
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:loopback=true
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=251,dl_vlan=1,dl_dst=C8:0A:A9:04:49:1A,actions=normal
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=252,ip,nw_dst=10.10.10.1,actions=set_field:1-\>vlan_vid,set_field:C8:(
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=4097,actions=output:1
```

1. The port will be always be "linkup" because it is a loopback port
2. Add loopback config in interface options for phyical ports and lag ports at ovs mode.
3. Due to different switch's chip are different, so some switch loopback port can send out packets, and others can not.
4. This function in crossflow mode should be added by xorplus.

Configuring ovs Remotely

Configuring ovsdb Locally

User can check the status of the **ovsdb-server** process using the **ps** command from the Linux shell.

```
admin@PicOS-OVS$ps aux|grep ovs
root      3422  0.0  0.1   7020  2788 ?        S    10:42   0:00 ovsdb-server /ovs/ovs-vswitchd.conf.db /tmp/invent
root      3435 15.7  1.5 122860 32320 ?        Sl   10:42   2:12 ovs-vswitchd --pidfile=ovs-vswitchd.pid --overwri
root      3494  0.0  0.2  12960  5752 ?        Ss   10:43   0:00 /usr/bin/python /ovs/share/openvswitch/scripts/ovs
admin     3738  0.0  0.0   2200   684 ttyS0    S+   10:56   0:00 grep --color=auto ovs
admin@PicOS-OVS$
```

The string '--remote=ptcp:6640:127.0.0.1' in the output above shows that the **ovsdb-server** is listening the local IP 127.0.0.1 and port 6640.

User can configure **ovs-vswitchd** locally as shown below:

```
root@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1 -- set interface te-1/1/1 type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
root@PicOS-OVS$ovs-vsctl set-controller br0 tcp:10.10.51.51:6633
```

Configuring ovsdb Remotely

Check the state of **ovsdb-server** on the switch.

```
admin@PicOS-OVS$ps aux|grep ovs
root      3422  0.0  0.1   7020  2788 ?        S    10:42   0:00 ovsdb-server /ovs/ovs-vswitchd.conf.db /tmp/invent
root      3435 14.9  1.5 122860 32388 ?        Sl   10:42   3:16 ovs-vswitchd --pidfile=ovs-vswitchd.pid --overwri
root      3494  0.0  0.2  12960  5752 ?        Ss   10:43   0:00 /usr/bin/python /ovs/share/openvswitch/scripts/ovs
admin     3835  0.0  0.0   2200   680 ttyS0    S+   11:04   0:00 grep --color=auto ovs
```

The string '--remote=db:Open_vSwitch,Manager,target' in the output above shows that the **ovsdb-server** is listening remote Manager and target default. User can configure switch ovsdb at remote side.

User can configure **ovs-vswitchd** remotely as shown below, switch's managerment ip is 10.10.51.138.

```
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.138:6640 add-br br0 -- set bridge br0 datapath_type=pica8
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.138:6640 add-port br0 te-1/1/1 vlan_mode=trunk tag=1 -- set interface te
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.138:6640 add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan op
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.138:6640 set-controller br0 tcp:10.10.51.51:6633
```

Add flow locally

User can add flow entry in switch cli.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,actions=output:32
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=29, cookie=0x0, duration=3.313s, table=0, n_packets=n/a, n_bytes=3481169152, in_port=31 actions=output:32
admin@PicOS-OVS$
```

Add flow remotely

User can add flow entry at remote side, and must configure controller before, switch's managerment ip is 10.10.51.138.

```
Switch,
admin@PicOS-OVS$ovs-vsctl set-controller br0 ptcp:6633:10.10.51.138
```

```
Remote server,
root@dev-42:~# ovs-ofctl add-flow tcp:10.10.51.138:6633 in_port=32,actions=output:31
root@dev-42:~#
```

Configuring ports in bridge

Adding ports in bridge

Adding access port

In the example below, the user creates a bridge named **br0,** using the **set bridge** command. With the **add-port** command, add access ports, **ge-1/1/1** and **ge-1/1/2**, to **br0**. The default PVID for both ports is 1.

```
root@PicOS-OVS$ovs-vsctl add-br br0
root@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=access tag=1 -- set Interface ge-1/1/1 type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=access tag=1 -- set Interface ge-1/1/2 type=pica8
root@PicOS-OVS$
```

If the user wants to allow use of a DAC line, user should enable DAC.

```
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/49 vlan_mode=access tag=1 -- set Interface te-1/1/49 type=pica8 optio
```

Adding Trunk Port

PicOS supports 802.1Q trunk ports (since PicOS 2.1). Each port has a default VLAN-ID; and by default, the VLAN-ID is 1. If user wants a port to belong to more than one VLAN, use the **vlan mode=trunk** command. When user specifies one port to a trunk port (tag=1), this port is the trunk port, the PVID is the tag number, and this port belongs to all the other VLANs (2-4094).

In the example below, the user specifies the VLAN mode to equal *trunk,* and then specifies the VLANs in the trunks:

```
root@PicOS-OVS$ ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 trunks=1000 -- set Interface ge-1/1/4 type=p
root@PicOS-OVS$
```

Setting the Port Link Speed

The trunk port can carry all VLANs if the user does not specify the *trunks* field, as shown below.

```
root@PicOS-OVS$ ovs-vsctl add-port br0 te-1/1/49 vlan_mode=access tag=1 -- set Interface te-1/1/49 type=pica8 optic
root@PicOS-OVS$
```

Modify port ofport

PicOS support modify port ofport,for example,modify ofport of te-1/1/69 from 69 to 190.

```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/69 ofport_request=190
admin@PICOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2):
dpid:0x1c488cea1b174fc4(2038033768489897924)
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
70(te-1/1/70): addr:8c:ea:1b:17:4f:c4
config: 0
state: LINK_UP
current: 10GB-FD FIBER
advertised: 1GB-FD 10GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 10000 Mbps now, 10000 Mbps max
190(te-1/1/69): addr:8c:ea:1b:17:4f:c4
config: 0
state: LINK_UP
current: 10GB-FD FIBER
advertised: 1GB-FD 10GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 10000 Mbps now, 10000 Mbps max
```

Setting FEC in port

Introduction

Forwarding Error Correction (FEC) is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The sender sends the data together with a certain redundant error correction code. When the data is received at the receiver's end, it is checked according to the error correction code. If an error is found, the receiver recognizes it and corrects the error without data retransmission.

The FEC function can be applied to 100G, 40G and 25G ports of the switch and works only when all of the three following conditions are matched:

- FEC function is enabled on both ends of the link.
- Optical modules are plugged in.
- Interface rate is auto or at the default value, i.g. 100G optical port works at 100Gb/s.

PICOS offers FEC algorithm RS-FEC (CL91) on 100G port and FEC BASE-R (CL74) on 40G port.

For 25G port, PICOS offers two different FEC algorithms on different switch platforms:

Trident 3, Maverick2, Helix5 and Tomahawk 2 platform switches support RS-FEC (CL108) mode, Tomahawk+/Tomahawk platform switches support BASE-R (CL74) mode.

> **NOTE:**
> The port can link up only when the FEC configurations and the FEC algorithm mode on both ends of the link are the same.

Configuration Example

```
root@PicOS-OVS$ ovs-vsctl add-port br0 xe-1/1/1 -- set Interface xe-1/1/1 type=pica8 options:use_fec=true
root@PicOS-OVS$
root@PicOS-OVS$ ovs-vsctl add-port br0 xe-1/1/1 -- set Interface xe-1/1/1 type=pica8 options:use_fec=false
root@PicOS-OVS$
```

Add Bond Ports

PicOS supports bond multiple ports as in_port or output, and this virtual port does not influence each physical port's forwarding packets. That mean the physical port which adds in bond port also can be configured as lag/gre/l2gre/vxlan and others.

Bonding port ge-1/1/1 ~ ge-1/1/4 as one port.

```
// add portsovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set Interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set Interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set Interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 -- set Interface ge-1/1/4 type=pica8

// add bond ports
ovs-vsctl add-port br0 bond1 -- set Interface bond1 type=pica8_bond
ovs-vsctl set Interface bond1 options:members=ge-1/1/2,ge-1/1/3,ge-1/1/4

// add flows
ovs-ofctl add-flow br0 in_port=2049,actions=1
ovs-ofctl add-flow br0 in_port=1,actions=2049
```

Port other_config

STP:

```
admin@PicOS-OVS$ovs-vsctl set port te-1/1/1 other_config:stp-path-cost=10
admin@PicOS-OVS$ovs-vsctl set port te-1/1/1 other_config:stp-port-num=20
admin@PicOS-OVS$ovs-vsctl set port te-1/1/1 other_config:stp-port-priority=255
```

Interface options

1)Interface options:

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:link_speed=1G
```

Note:speed value support to configure 40G,100G,25G,10G,1G,100M,10M and auto.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:mtu=1500
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 options:flow_ctl=tx_rx
```

Note:flow control value support tx,rx,tx_rx and none.

```
admin@PicOS-OVS$ovs-vsctl set interface he-1/1/1 options:use_fec=true
```

2)LACP:

```
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lag_type=lacp
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:members=ge-1/1/1,ge-1/1/2
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lacp-system-id=00:11:11:11:11:11
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lacp-time=fast | slow
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lacp-system-priority=32768
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lacp-mode=active | passive
admin@PicOS-OVS$ovs-vsctl -- set Interface te-1/1/1 options:lacp-port-id=2
admin@PicOS-OVS$ovs-vsctl -- set Interface te-1/1/1 options:lacp-port-priority=32768
admin@PicOS-OVS$ovs-vsctl -- set Interface te-1/1/1 options:lacp-aggregation-key=0
```

3)LFS:

```
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 options:link-fault-signaling=ignore-none
```

Note:it support ignore-none, ignore-local, ignore-remote and ignore-both.

```
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 options:up-mode=true
```

4)Tpid

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:tpid=0x8100
```

Note:tpid support 0x8100,0x88a8,0x9100 and 0x9200.

5)Access-vport

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:access-vport=true
```

Note:default value is false.

6)Loop the traffic which out from switch back to switch again.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:loopback=true
```

7)Tunnel:

Gre:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.60.10 opt
```

L2gre:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.
```

vxlan:

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.
```

8)Bond:

```
admin@PicOS-OVS$ovs-vsctl set Interface bond1 options:members=te-1/1/1,te-1/1/2
```

9)Lag:

```
admin@PicOS-OVS$ovs-vsctl set Interface ae1 options:lag_selected_min=1
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:lag_type=static
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_dst
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_src_dst
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_src
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_dst
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_src_dst
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_src
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=resilient
```

```
admin@PicOS-OVS$ovs-vsctl -- set Interface ae1 options:hash-mapping=advance
```

Note:default hash mapping is dl_src_dst.

10) Enable CDR function:

```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/1 options:cdr-admin-state=true/false
```

11)PTP

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:ptp-mode=e2etransparent
```

Interface other_config

Cfm:

```
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_extended=true
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_demand=true
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_interval=10000
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_ccm_vlan=2000
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_ccm_vlan=random
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_ccm_pcp=7
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 other_config:cfm_opstate=up/down
```

Configuring the Duplex Mode of Optical Port as Auto-negotiation Mode

Notes:

- Currently, duplex mode for optical port is only available for the 10 optical port when its port rate set to 1G.
- Duplex mode for optical port currently only supports to configure as auto, i.e. auto-negotiation mode.

```
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 options:link_speed=1G
admin@PicOS-OVS$ovs-vsctl set Interface te-1/1/1 options:duplex=auto
```

Configuring Port Breakout

Notes:

You need to restart or reboot the system to make the setting take effect when performing port breakout operation.

The following command configures port breakout for port with number 49.

```
admin@PICOS:~$ ovs-vsctl set-port-breakout 49 true
  Port 49 has been set breakout=true!
  Please reboot for the change to take effect!
admin@PICOS:~$ sudo systemctl restart picos
```

The following command disables port breakout for port with number 49.

```
admin@PICOS:~$ ovs-vsctl set-port-breakout 49 false
  Port 49 has been set breakout=false!
  Please reboot for the change to take effect!
admin@PICOS:~$ sudo systemctl restart picos
```

Configuring TPID in Port

PicOS support push/swap/pop S-VLAN in Q-in-Q, and the S-VLAN TPID can configure as 0x8100/0x88a8/0x9100 and 0x9200. But in the same port, PicOS only support configure one TPID value, that means the traffic through one port will can push/swap/pop one type of TPID.

a, If one TPID configured in ingress port, switch can recognize it and deal the matched traffic;

b, If one TPID configured in egress port, switch can design it in the traffic which send out from the port.

1, TPID used in Q-in-Q

> ⚠ If the actions include push-vlan and has no push_l2mpls:
>
> push_vlan action will use out_port's tpid.
>
> For example,
>
> a. untagged packet push one tag, the result will be: out_port's tpid | payload
>
> b. untagged packet push two tags, the result will be: out_port's tpid | 0x8100 | payload

Once configure TPID in port, need reboot switch.Command:

```
ovs-vsctl set interface <port> options:tpid=<value>

<value> can configure mutiple values such as 0x8100/0x88a8/0x9100/0x9200, for example if the S-VLAN TPID is 0x88a8,
By default, the value is 0x8100.
```

In Q-in-Q flow, only support match outer-vlan.

Push-vlan: Design TPID during push S-VLAN, need configure TPID in egress.

Example:

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:tpid=0x8100
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:tpid=0x88a8

Push one vlan:
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan=0x88a8,set_field:1234-\>vlan_vid,output:2

Push two vlans,
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=push_vlan=0x8100,set_field:10-\>vlan_vid,push_vlan=0x88a8,
```

Swap-vlan: Match TPID in ingress port and design TPID in egress port, so need configure TPID in ingress and egress.

Example:

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:tpid=0x88a8
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/2 options:tpid=0x88a8

admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_vlan=10,actions=set_field:100-\>vlan_vid,output:2
```

Pop-vlan: Match TPID in ingress port, need configure TPID in ingress port.

Example:

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:tpid=0x88a8

admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_vlan=10,actions=pop_vlan,output:2
```

2, TPID used in push L2MPLS

This feature means push/swap/pop vlan before push L2MPLS. It is simmilar with Q-in-Q, but operation is different from Q-in-Q.

> ⚠ 1, This feature only support in platform 3922 and 3924;
>
> 2, If user want use TPID before push L2MPLS, must configure TPID on ingress port.

3, push_vlan action before push_l2mpls will use in_port's tpid, and push_vlan action in push_l2mpls will use out_port's tpid. One case need to note is that if only one tag exist before l2mpls, its tpid should be 0x8100.

For example,

a. untagged packet push one tag and then push l2mpls, the result will be: l2mpls | 0x8100 | payload

b. untagged packet push two tags and then push l2mpls, the result will be: l2mpls | in_port's tpid | 0x8100 | payload

a, No mather push/swap/pop vlan before push L2MPLS, TPID must configure in ingress port.

Once configure TPID in port, need reboot switch.Command:

```
ovs-vsctl set interface <port> options:tpid=<value>

<value> can configure one value as 0x8100/0x88a8/0x9100/0x9200, for example if the S-VLAN TPID is 0x88a8, the valu
By default, the value is 0x8100.
```

Push-vlan: Configure TPID in ingress port.

Example: The push_vlan and push_l2mpls are performed in network ingress side. In network egress side, PicOS switch just pop_l2mpls. In this example, we only care the network ingress side.



a, At the Ingress side, matching in_port and untag, actions: push_svlan (TPID 0x8100/0x88a8/0x9100/0x9200) push_cvlan(TPID 0x8100) then push l2mpls.

```
ovs-vsctl set interface te-1/1/11 options:tpid=0x88a8
ovs-ofctl add-flow br-iris "in_port=11,vlan_vid=0x0000/0x1fff,actions=push_vlan:0x88a8,set_field:100->vlan_vid,pus
```

b, At the Ingress side, cvlan (TPID=0x8100) then push_l2mpls.

```
ovs-vsctl set interface te-1/1/11 options:tpid=0x88a8
ovs-ofctl add-flow br-iris "in_port=11,vlan_vid=0x0000/0x1fff,actions=push_vlan:0x8100,set_field:10->vlan_vid,push_
```

If want match untag packets, the flow entry should include match vlan_vid=0x0000/0x1fff, and must set option-match-vlan-type is true.

admin@PicOS-OVS$ovs-vsctl set-option-match-vlan-type true

Swap-vlan: Configure TPID in ingress port.

Example: Swap and push_l2mpls are performed in network ingress side. In egress side, PicOS switch just pop_l2mpls. In this example, we only care the network ingress side.



a, At the **Ingress** side, matching in_port and S-VLAN/C-VLAN (C-VLAN TPID support 0x8100, S-VLAN TPID support 0x8100/0x88a8/0x9100/0x9200), actions: swap S-VLAN and C-VLAN;

```
ovs-vsctl set interface te-1/1/11 options:tpid=0x88a8
ovs-ofctl add-flow br-iris "in_port=11,vlan_tci=0x1032,inner_vlan_tci=0x100a,actions=set_field:100->vlan_vid,set_f
```

b, swap S-VLAN only or swap C-VLAN , then push_l2mpls.

```
ovs-vsctl set interface te-1/1/11 options:tpid=0x88a8
ovs-ofctl add-flow br-iris "in_port=11,vlan_tci=0x1032,inner_vlan_tci=0x1000/0x1000,actions=set_field:100->vlan_vi

ovs-ofctl add-flow br-iris "in_port=11,vlan_tci=0x1000/0x1000,inner_vlan_tci=0x1000/0x1000,actions=set_field:100->
```

Pop_vlan: Configure TPID in ingress port.

Example: The pop_vlan and push_l2mpls are performed in network ingress side. In egress side, PicOS switch just pop_l2mpls. In this example, we only care the network ingress side.



At the Ingress side, matching in_port and S-VLAN/C-VLAN, actions: pop S-VLAN or pop S-VLAN and C-VLAN, then push_l2mpls.

```
ovs-vsctl set interface te-1/1/11 options:tpid=0x88a8
ovs-ofctl add-flow br-iris "in_port=11,vlan_tci=0x1032,inner_vlan_tci=0x100a,actions=pop_vlan,pop_vlan,push_l2mpls
```

Configuring LAG and LACP

- Adding LAG and LACP
- GTP hash
- Lag hash
- Lag Resilient hash
- Symmetric Hashing in lag and ecmp

Adding LAG and LACP

LAG/LACP

Link aggregation (LAG) refers to *aggregating* multiple physical network links in parallel in order to increase throughput beyond what a single link could sustain, and provide redundancy in case any of the links should fail.

Link Aggregation Control Protocol (LACP) refers to bundling of several physical ports together to form a single logical channel. Network devices use LACP to negotiate automatic bundling of links by sending LACP packets to its directly connected peer(s)

LACP features and practical examples:

1. Maximum number of bundled ports allowed in the port channel: valid values are from 1 to 8.
2. LACP packets are sent with a well known multicast group MAC address 01:80:c2:00:00:02
3. LACP detection period:
    - LACP packets are transmitted every second
    - Keep alive mechanism for link members: (default: slow = 30s, fast=1s)
4. LACP can have the port-channel load-balance mode:
    - load-balancing can be configured using a combination of in_port, L2, L3 and L4 headers.
5. LACP mode:
    - active: Enables LACP unconditionally.
    - passive: Enables LACP only when an LACP device is detected. (This is the default state)

1, PicOS OVS supports LAG and LACP.

2, PicOS can support 48 LAG or LACP at most. Each LAG has a maximum of 8 member ports.

3, The port ranges in PicOS are as follows:

Port Type	Port Number
LAG	1025-2047

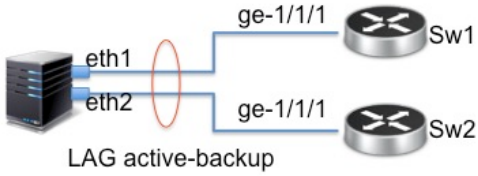
Create a Static LAG

In following configuration, user can create LAG ae1, and add port 2 and port 3 into this LAG

```
root@PicOS-OVS# ovs-vsctl  add-port br0 ae1 vlan_mode=trunk tag=1 -- set Interface ae1 type=pica8_lag
root@PicOS-OVS# ovs-vsctl -- set Interface ae1 options:lag_type=static
root@PicOS-OVS# ovs-vsctl -- set Interface ae1 options:members=ge-1/1/2,ge-1/1/3
```

Dual Homing a Host

While dual-homing a host does not require a LAG configuration on the switch, this configuration illustrates steps required to setup LAG on the host connected to two different switches.



Host LAG Configuration	Switch Port Configuration
pica8@Ubuntu$ more /etc/modprobe.d/bonding.conf bonding mode=1 miimon=100 pica8@Ubuntu$ more /etc/network/interfaces # NIC bonding config for LAG active-backup START auto eth1 iface eth1 inet manual	OVS-Sw1$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set interface ge-1/1/1 type=pica8 OVS-Sw2$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set interface ge-1/1/1 type=pica8

Host LAG Configuration	Switch Port Configuration
bond-master bond0 bond-primary eth1 auto eth2 iface eth2 inet manual bond-master bond0 auto bond0 iface bond0 inet static address 10.0.0.20 netmask 255.255.255.0 bond-mode active-backup bond-miimon 100 bond-slaves none # NIC bonding config for LAG active-backup END pica8@Ubuntu$ cat /proc/net/bonding/bond0 Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011) Bonding Mode: fault-tolerance (active-backup) Primary Slave: eth1 (primary_reselect always) Currently Active Slave: eth1 MII Status: up MII Polling Interval (ms): 100 Up Delay (ms): 0 Down Delay (ms): 0 Slave Interface: eth2 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 0 Permanent HW addr: 00:0c:29:70:2e:c2 Slave queue ID: 0 Slave Interface: eth1 MII Status: up Speed: 1000 Mbps Duplex: full Link Failure Count: 0 Permanent HW addr: 00:0c:29:70:2e:b8 Slave queue ID: 0	

Create a LACP Port

Following is the configuration on the host (running Ubuntu):

```
pica8@Ubuntu:~$ more /etc/modprobe.d/bonding.conf
bonding mode=4 miimon=100 lacp_rate=1

pica8@Ubuntu:~$ more /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
auto eth0
iface eth0 inet dhcp

# NIC bonding config with LACP START
auto eth1
iface eth1 inet manual
        bond-master bond0
auto eth2
iface eth2 inet manual
        bond-master bond0
auto bond0
iface bond0 inet static
 address 10.0.0.10
 netmask 255.255.255.0
bond-mode 802.3ad
bond-miimon 100
bond-lacp-rate 1
bond-slaves none
# NIC bonding config with LACP END


pica8@Ubuntu:~$ sudo systemctl restart networking

pica8@Ubuntu:~$ cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

802.3ad info
LACP rate: fast
Min links: 0
Aggregator selection policy (ad_select): stable
Active Aggregator Info:
Aggregator ID: 3
Number of ports: 2
Actor Key: 17
Partner Key: 1
Partner Mac Address: 00:11:11:11:11:11

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:fd:75:ae
Aggregator ID: 3
Slave queue ID: 0

Slave Interface: eth2
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:fd:75:b8
Aggregator ID: 3
Slave queue ID: 0
```

Following is the LACP configuration on the switch.

The default (slow) LACP timer is 30s whereas fast timer is 1s. LACP mode determines which node initiates the negotiation: active sets the switch to initiate the LACP handshake, while in passive mode the switch accepts all incoming LACP requests.

```
admin@PicOS-OVS$ ovs-vsctl  add-port br0 ae1 vlan_mode=trunk tag=1 -- set Interface ae1 type=pica8_lag
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:lag_type=lacp
```

```
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:members=ge-1/1/1,ge-1/1/2
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:lacp-system-id=00:11:11:11:11:11
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:lacp-time=fast | slow


Optional Settings:
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:lacp-system-priority=32768
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ae1 options:lacp-mode=active | passive
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ge-1/1/2 options:lacp-port-id=2
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ge-1/1/2 options:lacp-port-priority=32768
admin@PicOS-OVS$ ovs-vsctl  -- set Interface ge-1/1/2 options:lacp-aggregation-key=0
```

From PicOS version 2.7.1, support is added to configure minimum number port in a LACP or LAG. The command is as follows:

`ovs-vsctl set Interface <lag port> options:lag_selected_min=<value>`

```
admin@PicOS-OVS$ovs-vsctl set Interface ae1 options:lag_selected_min=1
```

Create Static Flow for LAG or LACP

In following configuration, user can create static flow whose output port is a LAG or LACP.

```
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1025,actions=output:1
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:1025
```

LAG number index is shown as following:

LAG Name	LAG Number
ae1	1025
ae2	1026
..	..
ae1023	2047

Display the LACP Information

User can display the LACP information with the following CLI commands.

```
admin@PicOS-OVS$ovs-appctl lacp/show

---- ae1 ----
status: active negotiated
sys_id:00:11:11:11:11:11
sys_priority: 32768
aggregation key: 1
lacp_time: fast
slave: ge-1/1/1: current attached
port_id: 1
port_priority: 32768
may_enable: true
actor sys_id:00:11:11:11:11:11
actor sys_priority:32768
actor port_id: 1
actor port_priority:32768
actor key: 1
actor state: activity timeout synchronized collecting distributing
partner sys_id:00:0c:29:fd:75:b8
partner sys_priority:65535
partner port_id: 2
partner port_priority:255
partner key: 17
partner state:activity timeout aggregation synchronized collecting distributing
```

```
slave: ge-1/1/2: current attached
port_id: 1
port_priority: 32768
may_enable: true
actor sys_id:00:11:11:11:11:11
actor sys_priority:32768
actor port_id: 1
actor port_priority:32768
actor key: 1
actor state: activity timeout synchronized collecting distributing
partner sys_id:00:0c:fe:ae:69:ac
partner sys_priority:65535
partner port_id: 2
partner port_priority:255
partner key: 17
partner state:activity timeout aggregation synchronized collecting distributing
```

LAG speed

From PicOS version 2.7.2, support for LAG speed has been added. User can check the LAG speed configuration with the command **"ovs-ofctl show br0 ".**

Examples

Topology

ge-1/1/1----------connect ixia1

ge-1/1/2----------connect ixia2

ge-1/1/3----------connect ixia3

ge-1/1/4----------connect ixia4

Step 1: Create a bridge and add four ports (PX1,PX2,PX3)

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 -- set interface ge-1/1/4 type=pica8
```

Step 2: Add a lag port

```
ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:members=ge-1/1/2,ge-1/
ovs-vsctl -- set interface ae1 options:lag_type=static
```

Check the lag port speed

```
ovs-ofctl show br0
check "1025(ae1).*state.* LINK_UP"
check "speed.*300 Mbps"
```

Step 3: Add flow

```
ovs-ofctl add-flow br0 in_port=1,actions=output:1025
 check the flows:
ovs-ofctl dump-flows br0
check "in_port=1"
ovs-appctl pica/dump-flows
check "in_port=1"
```

Step 4: Send ipv4 packets and check the result

(1) Send no changing packets to PX1,(dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22,dl_vlan=10,ip,nw_src=192.168.1.10,nw_dst=192.168.2.10)

Result:

```
then PX2,PX3 or PX4 will transmit all the packets.
```

```
Check:
dl_src: 22 11 11 11 11 11
dl_dst:22 22 22 22 22 22
offset:30
ip:C0 A8 01 0A C0 A8 02 0A
```

(2)sending increasing src mac to PX1, (dl_src=22:11:11:11:11:11(increase),dl_dst=22:22:22:22:22:22,dl_vlan=10,ip,nw_src=192.168.1.10,nw_dst=192.168.2.10)

Result:

```
then both PX2, PX3 and PX4 will transmit the packets.
Check:
dl_dst:22 22 22 22 22 22
offset:30
ip:C0 A8 01 0A C0 A8 02 0A
```

Step 5: Down one or more port of lag and check the lag speed

(1)ovs-ofctl mod-port br0 ge-1/1/2 down

```
ovs-ofctl show br0
check "1025(ae1).*state.* LINK_UP"
check "speed.*200Mbps"
```

(2)ovs-ofctl mod-port br0 ge-1/1/3 down

```
ovs-ofctl show br0
check "1025(ae1).*state.* LINK_UP"
check "speed.*100Mbps"
```

(3)ovs-ofctl mod-port br0 ge-1/1/4 down

```
ovs-ofctl show br0
check "1025(ae1).*state.* LINK_DOWN"
check  "speed.*0Mbps"
```

Step 6: Up all the ports of lag and check the lag speed

```
ovs-ofctl mod-port br0 ge-1/1/2 up
ovs-ofctl mod-port br0 ge-1/1/3 up
ovs-ofctl mod-port br0 ge-1/1/4 up
ovs-ofctl show br0
check "1025(ae1).*state.* LINK_UP"
check "speed.*300Mbps"
```

Step 7: Test end and clear the configure

```
ovs-vsctl del-br br0
```

GTP hash

From 2.9.1.3,GTP hash is supported on pica8 switch.GTP hash support ecmp-gtp-hash and lag-gtp-hash.GTP teid hash works well whatever adding a lag port or lag-select-group.But only works well when configure ecmp-select-group.The layer4 port hash fields does not work when setting with gtp_teid(ovs-vsctl set-lag-advance-hash-mapping-fields gtp_teid port_src),but works well when not set gtp_teid(ovs-vsctl set-lag-advance-hash-mapping-fields port_src).You can modify the udf dst port through this commnad "ovs-vsctl set-gtp-udp-dst-ports <portnumber>",default is 2152.After enable advance mode on lag port,all hash fields are enabled except gtp_teid.The same with the ecmp-hash-fields.

support platforms
TridentII, tridentII+,thomahawk support gtp hash

Command
1. hash through a lag port
step1,add a lag port
ovs-vsctl add-port br0 te-1/1/4 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/5 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:members=te-1/1/4,te-1/1/5
step2,set hash-fields to teid
ovs-vsctl set interface ae1 options:hash-mapping=advance
ovs-vsctl set-lag-advance-hash-mapping-fields gtp_teid
step3,add a flow
without matching teid
ovs-ofctl add-flow br0 in_port=3,actions=1025
matching teid
ovs-vsctl set-udf-mode "udf0(l4,offset=12,length=4)"
ovs-ofctl add-flow br0 in_port=1,table=250,udf0=0x00000000/0xffffffff0,actions=1025
2. lag-select-group
step1,enable lag-select-group and add a group
ovs-vsctl set-group-ranges lag-select-groups=2-20
sudo systemctl restart picos

ovs-ofctl add-group br0 group_id=2,type=select,bucket=output:4,bucket=output:5
step2,set hash-fields to teid
ovs-vsctl set-lag-advance-hash-mapping-fields gtp_teid
step3,add a flow
without matching teid
ovs-ofctl add-flow br0 in_port=3,actions=group:2
with matching teid:
ovs-vsctl set-udf-mode "udf0(l4,offset=12,length=4)"
ovs-ofctl add-flow br0 in_port=1,table=250,udf0=0x00000000/0xffffffff0,actions=group:2
3. ecmp-select-group
step1,enable ecmp-select-group and add a group
ovs-vsctl set-group-ranges ecmp-select-groups=1-100

sudo systemctl restart picos

ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38

Step2, enable ecmp-udf-hash and configure hash-fields is gtp_teid.

ovs-vsctl set-l3-ecmp-hash-fields gtp_teid

Step3, add a flow

ovs-ofctl add-flow br0 in_port=1,actions=group:1

Lag hash

Lag Hash Configuration

Lag hash commands are as follows.

```
# Config command
ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_dst
ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_src_dst
ovs-vsctl -- set Interface ae1 options:hash-mapping=dl_src
ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_dst
ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_src_dst
ovs-vsctl -- set Interface ae1 options:hash-mapping=nw_src
ovs-vsctl -- set Interface ae1 options:hash-mapping=resilient
ovs-vsctl -- set Interface ae1 options:hash-mapping=advance
ovs-vsctl -- set-lag-advance-hash-mapping-fields dl_dst dl_src ether_type in_port nw_dst nw_proto nw_src port_dst p
vlan
# Show command
ovs-vsctl show-lag-advance-hash-mapping-fields
```

If not special the hash-mapping in one lag interface, dl_src_dst will be set by default; And if not special the hash-mapping in set-lag-advance-hash-mapping-fields, all field will be set.

Lag Resilient hash

From 2.9.2,pica8 switch support lag resilient hash. If one port removed from the lag or link_down,the traffic of this port will hash to the other ports of the lag without affect orignal traffic of the other ports.

Command

ovs-vsctl -- set Interface ae1 options:hash-mapping=resilient: Once enable resilient hash,all the hash fields in advance mode are enabled by default.

ovs-vsctl set-max-resilient-hash-lag-count COUNT : the valid value of COUNT is 1, 2, 4, 8, 16, 32, 64; The default value is 1.The COUNT means the max count of lags which can be set to resilient hash.

support platform
At present, trident2, trident2 plus support resilient hash.Eg:4048,4806,P5401,P5101,as5712,AS6701_32x,as6712_32x,as5812

Example

set hash-mapping-fields to mac,ip,vlan

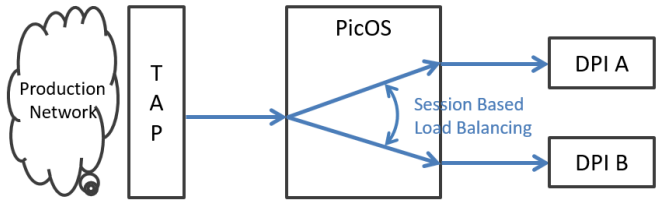
Test Name	Test basic flow
Test Configuration	
Test Procedure	**Step1:configure bridge and port** ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8 ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1 -- set interface te-1/1/1 type=pica8 ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1 -- set interface te-1/1/2 type=pica8 ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1 -- set interface te-1/1/3 type=pica8 ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 – set interface ae1 type=pica8_lag options:members=te-1/1/2,te-1/1/3,te-1/1/4 options:lag_type=static ovs-vsctl -- set Interface ae1 options:hash-mapping=resilient **step2:add flow** ovs-ofctl add-flow br0 in_port=1,actions=1025 **step3:set hash-mapping-field to dl_dst:** ovs-vsctl set-lag-advance-hash-mapping-fields dl_dst **Send 12packets/sec ipv4 packets to te-1/1/1,with different dst mac(22:22:22:22:22:10 to 22:22:22:22:22:15):** MAC: Destination Address : 22 22 22 22 22 10 MAC: Source Address : 22 11 11 11 11 40 Vlan----------20 **Te-1/1/2,te-1/1/3,te-1/1/4 will transmit the packets,eg:te-1/1/2 transmit packets with dst mac 22:11:11:11:11:10,13,15,te-1/1/3 transmit packets with dst mac 11,14,te-1/1/4 transmit packets with dst mac 12.** **send 12packets/sec ip packets with src ip increasement to te-1/1/1,then one of the lag port transmit all the packets.** **Down te-1/1/2 then the traffic of te-1/1/2 will be hash to te-1/1/3 and te-1/1/4, the original traffic of te-1/1/3 and te-1/1/4 will not be redistribute.** **Then up the te-1/1/2 port, the traffic of te-1/1/2 is some traffic of the other two ports.** **Step4:set hash-mapping-field to dl_src** ovs-vsctl set-lag-advance-hash-mapping-fields dl_src **Send 12packets/sec ipv4 packets to te-1/1/1,with different src mac(22:11:11:11:11:40 to 22:11:11:11:11:45):** MAC: Destination Address : 22 22 22 22 22 10 MAC: Source Address : 22 11 11 11 11 40 Vlan----------20 **Te-1/1/2,te-1/1/3,te-1/1/4 will transmit the packets,eg:te-1/1/2 transmit packets with dst mac 22:11:11:11:11:40,43,45,te-1/1/3 transmit packets with dst mac 41,44,te-1/1/4 transmit packets with dst mac 42.** **Down te-1/1/2 then the traffic of te-1/1/2 will be hash to te-1/1/3 and te-1/1/4, the original traffic of te-1/1/3 and te-1/1/4 will not be redistribute.** **Then up the te-1/1/2 port, the traffic of te-1/1/2 is some traffic of the other two ports** **Step5:set hash-mapping-field to nw_src** ovs-vsctl set-lag-advance-hash-mapping-fields nw_src **send 12packets/s contents with src ip 1.1.1.1-1.1.6:**

	MAC: Destination Address : 22 22 22 22 22 10 MAC: Source Address : 22 11 11 11 11 40 Vlan----------20 IP: Source Address = 1.1.1.1 **Te-1/1/2,te-1/1/3,te-1/1/4 will transmit the packets,eg:te-1/1/2 transmit packets with source ip 1.1.1.1 and 1.1.1.3. te-1/1/3 transmit packets with source ip 1.1.1.2 and 1.1.1.4 ,te-1/1/4 transmit packets with srouce ip 1.1.1.5 and 1.1.1.6.** **Down te-1/1/2 then the traffic of te-1/1/2 will be hash to te-1/1/3 and te-1/1/4, the original traffic of te-1/1/3 and te-1/1/4 will not be redistribute.** **Then up the te-1/1/2 port, the traffic of te-1/1/2 is some traffic of the other two ports** **Step6:set hash-mapping-field to nw_dst** ovs-vsctl set-lag-advance-hash-mapping-fields nw_dst **send 12packets/s contents with dst ip 4.4.4.1-4.4.4.6:** MAC: Destination Address : 22 22 22 22 22 10 MAC: Source Address : 22 11 11 11 11 40 Vlan----------20 IP: Source Address = 1.1.1.1 IP: dst Address = 4.4.4.1 **Te-1/1/2,te-1/1/3,te-1/1/4 will transmit the packets,eg:te-1/1/2 transmit packets with dst ip 4.4.4.1 and 4.4.4.3. te-1/1/3 transmit packets with source ip 4.4.4.2 and 4.4.4.4 ,te-1/1/4 transmit packets with srouce ip 4.4.4.5 and 4.4.4.6.** **Down te-1/1/2 then the traffic of te-1/1/2 will be hash to te-1/1/3 and te-1/1/4, the original traffic of te-1/1/3 and te-1/1/4 will not be redistribute.** **Then up the te-1/1/2 port, the traffic of te-1/1/2 is some traffic of the other two ports** **Step6:set hash-mapping-field to vlan** ovs-vsctl set-lag-advance-hash-mapping-fields vlan **send 12packets/s contents with vlan from 20 to 25** **send 12packets/s contents with vlan20-25:** MAC: Destination Address : 22 22 22 22 22 10 MAC: Source Address : 22 11 11 11 11 40 Vlan----------20 IP: Source Address = 1.1.1.1 IP: dst Address = 4.4.4.1 **Te-1/1/2,te-1/1/3,te-1/1/4 will transmit the packets,eg:te-1/1/2 transmit packets with vlan20,22. te-1/1/3 transmit packets with vlan 21 ,te-1/1/4 transmit packets with vlan 23,24,25.** **Down te-1/1/3 then the traffic of te-1/1/3 will be hash to te-1/1/2 or te-1/1/4, the original traffic of te-1/1/2 and te-1/1/4 will not be redistribute.** **Then up the te-1/1/3 port, the traffic of te-1/1/3 is some traffic of the other two ports.**

Symmetric Hashing in lag and ecmp

Summary

From PicOS2.9.1, OVS support Symmetric Hashing in LAG interface and ECMP interface.



Traffic from the production network is transferred to DPIs by session based load balancing.
Session based load balancing means same session uplink and downlink packets are transferred to same DPI.
In current image, the packets that are transferred to same DPI have same **IP addresses** and **L4 port numbers** symmetrically with each other.

> 1, Symmetric hashing is supported on Helix4 , Trident2, Trident2+, Trident3 and Tomahawk platform switches.
>
> 2, Symmetric hash key only include: ip address, ip address+l4 port number.
>
> 3, If the hash fields include other keys: mac address, vlan, etc. Symmetric hash will be influenced.

Command

Enable/Disable symmetric hash in lag interface

```
ovs-vsctl set-symmetric-hash lag true
ovs-vsctl set-symmetric-hash lag false
```

Except enable lag symmetric hash in glocal, user also need configure advance field in lag interface.

```
ovs-vsctl -- set Interface ae1 options:hash-mapping=advance
```

Configure IP addresses symmetrically in lag advance hash mapping fields.

```
ovs-vsctl set-lag-advance-hash-mapping-fields nw_dst nw_src
```

Configure IP addresses and L4 port numbers symmetrically in lag advance hash mapping fields.

```
ovs-vsctl set-lag-advance-hash-mapping-fields nw_dst nw_src port_src port_dst
```

Enable/Disable symmetric has in ecmp interface

```
ovs-vsctl set-symmetric-hash ecmp true
ovs-vsctl set-symmetric-hash ecmp false
```

Configure IP addresses symmetrically in l3 ecmp hash fields.

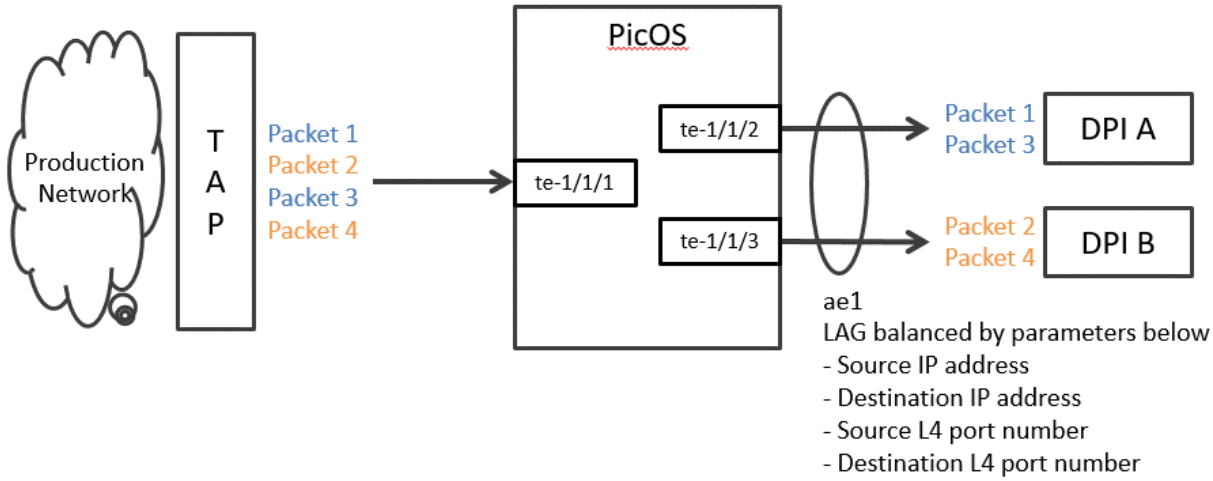
```
ovs-vsctl set-l3-ecmp-hash-fields nw_src nw_dst
```

Configure IP addresses and L4 port numbers symmetrically in l3 ecmp hash fields.

```
ovs-vsctl set-l3-ecmp-hash-fields nw_src nw_dst port_src port_dst
```

Example

1. Configure symmetric in lag interface.



The image of session-based load balancing like below:

Packet X (Src IP, Src Port, Dest IP, Dest Port)

Packet 1 (20.0.0.1, 10001, 10.0.0.1, 80) => output to te-1/1/2 of ae1

Packet 2 (20.0.0.1, 10002, 10.0.0.2, 80) => output to te-1/1/3 of ae1

Packet 3 (10.0.0.1, 80, 20.0.0.1, 10001) => output to te-1/1/2 of ae1

Packet 4 (10.0.0.2, 80, 20.0.0.1, 10002) => output to te-1/1/3 of ae1

-> Packet 1 and Packet 3 are the same session. So the 2 packets are transferred to same LAG member port.

-> Packet 2 and Packet 4 are the same session. So the 2 packets are transferred to same LAG member port.

```
1, Add bridge and ports.
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:members=te-1/1/2,te-1/

2, Configure advance hash mapping field and apply to ae1.
ovs-vsctl -- set Interface ae1 options:hash-mapping=advance
ovs-vsctl set-lag-advance-hash-mapping-fields nw_dst nw_src port_src port_dst


3, Enable lag symmetric.
ovs-vsctl set-symmetric-hash lag true

4, Add flow entry.
ovs-ofctl add-flow br0 in_port=1,actions=output:1025
```

2. Configure symmetric in ecmp interface.

```
1, Add bridge and ports.
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1

2, Configure ecmp group.
ovs-vsctl set-group-ranges ecmp-select-groups=1-10000

3, Configure l3 ecmp hash field.
ovs-vsctl set-l3-ecmp-hash-fields nw_src nw_dst port_src port_dst
```

```
4, Enable ecmp symmetric.
ovs-vsctl set-symmetric-hash ecmp true

5, add group and flow.
ovs-ofctl add-group br0 group_id=1,type=select,bucket=set_field:00:00:00:11:11:11-\>eth_src,set_field:00:00:00:22:
ovs-ofctl add-flow br0 in_port=1,actions=group:1
```

Configuring QoS

Configuring QoS scheduler

PicOS OVS Supports qos/queue

> 1, PicOS OVS support configure qos scheduler type: SP, RR, WRR, WFQ
>
> 2, In the PicOS switch, there are 7 queues in ASIC with priority 0~7 (In the current version, P3922/P3780/3920, only support queues 0~3). Queue 7 being the highest priority and queue 0 being the lowest priority.

Command:

Add qos

```
ovs-vsctl -- set port <interface name> qos=@<qos name1> -- --id=@<qos name1> create qos type=<scheduler type> queue
```

List qos and queue table

```
ovs-vsctl list qos
ovs-vsctl list queue
```

Check qos config in interface

```
ovs-appctl qos/show <interface>
ovs-ofctl queue-get-config br0 [port]
```

Check queue counter

```
ovs-ofctl queue-stats <bridge> [port]
```

Clear queue and qos

```
ovs-vsctl clear port <interface> qos
ovs-vsctl --all destroy qos
ovs-vsctl --all destroy queue
```

SP

In SP (short for Strict Priority) mode.

> 1, The SP queue has priority to be scheduled when work with others queue whether the queue priority is high or not.
>
> 2, If different flows from different input ports and enter the different queue on the one output port, and low priority queue has congestion, this time maybe appear **Head-of-line blocking.**

Example:

Flow (dl_src is 22:11:11:11:11:11) will be forwarded to queue 0 of port 3

Flow (dl_src is 22:11:11:11:11:12) will be forwarded to queue 7 of port 3.
Min and max rate of queue 0 and queue 7 is set as 10M

```
root@PicOS-OVS# ovs-ofctl del-flows br0
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=set_queue:0,output=3
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=2,dl_src=22:11:11:11:11:12,actions=set_queue:7,output=3
root@PicOS-OVS# ovs-vsctl -- set port ge-1/1/3 qos=@newqos -- --id=@newqos create qos type=PRONTO_STRICT queues:0=@
```

RR

RR(short for Round Robin) is a scheduler mode of Qos. It uses a round robin scheduling algorithm between the queues and can avoid the lowest priority queues not being serviced for long time when traffic congestion happens.

Example:

Add qos on interface te-1/1/5, and configure queue2 and queue3

```
ovs-vsctl -- set port te-1/1/5 qos=@newqos -- --id=@newqos create qos type=PRONTO_ROUND_ROBIN queues:2=@newqueue qu
```

WRR

WRR(short for Weighted Round Robin)is a scheduler mode of Qos. It uses a round robin scheduling algorithm between the queues and can avoid the lowest priority queues not being serviced for long time when traffic congestion happens. When you use WRR scheduling mode, you can define your own weighted value for each queue to distribute different service time for queue.Generaly,greater the weight, longer the serviced time.

Example:

1.1 Create a qos and add two queues (0 and 3)to qos for port te-1/1/3

```
root@PicOS-OVS$ovs-vsctl -- set port te-1/1/3 qos=@newqos -- --id=@newqos create qos type=PRONTO_WEIGHTED_ROUND_ROI
b41dbaab-dc60-40ff-8a11-7a241bfd5a5c
f7c5e8ff-f81f-4e69-9096-9b1251f29618
5d57cffb-b9b7-4324-9402-034ab9fac050
root@PicOS-OVS$
```

1.2 Flow config

```
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=set_queue:0,output=3
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=2,dl_src=22:11:11:11:11:12,actions=set_queue:3,output=3
root@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=18, cookie=0x0, duration=422.520s, table=0, n_packets=n/a, n_bytes=0, in_port=2,dl_src=22:11:11:11:11:12 a
 flow_id=17, cookie=0x0, duration=426.136s, table=0, n_packets=n/a, n_bytes=0, in_port=1,dl_src=22:11:11:11:11:11 a
root@PicOS-OVS$
root@PicOS-OVS$ovs-appctl pica/dump-flows
#10 normal permanent flow_id=17 in_port=1,dl_src=22:11:11:11:11:11, actions:3
#6 normal_d permanent flow_id=13 priority=0, actions:drop
#8 normal permanent flow_id=18 in_port=2,dl_src=22:11:11:11:11:12, actions:set(skb_priority(0x3)),3
Total 3 flows in HW.
root@PicOS-OVS$
```

notice: queue 0 is the default queue,the HW flow don't display it.

1.3 Result

Firstly,both the queue 0 and queue 7 should provides a minimum bandwidth guarantee (200M) during congestion, then each queue distribute the remaining packets according the queue weight .

2 Check qos

```
root@PicOS-OVS$ovs-vsctl list qos
_uuid               : b41dbaab-dc60-40ff-8a11-7a241bfd5a5c
external_ids        : {}
other_config        : {}
queues              : {0=f7c5e8ff-f81f-4e69-9096-9b1251f29618, 3=5d57cffb-b9b7-4324-9402-034ab9fac050}
type                : PRONTO_WEIGHTED_ROUND_ROBIN
root@PicOS-OVS$
```

3 Check one queue according to its queue-uuid.

```
root@PicOS-OVS$ovs-vsctl list queue 5d57cffb-b9b7-4324-9402-034ab9fac050
_uuid               : 5d57cffb-b9b7-4324-9402-034ab9fac050
dscp                : []
external_ids        : {}
other_config        : {min-rate="200000000", weight="3"}
root@PicOS-OVS$
```

4 Check qos of a port from hardware

```
root@PicOS-OVS$ovs-appctl qos/show te-1/1/3
QoS: te-1/1/3 PRONTO_WEIGHTED_ROUND_ROBIN
Default:
        burst: 0
        max-rate: 0
        min-rate: 200000000
        weight: 3
        tx_packets: 0
        tx_bytes: 0
        tx_errors: 0
Queue 3:
        burst: 0
        max-rate: 0
        min-rate: 200000000
        weight: 3
        tx_packets: 0
        tx_bytes: 0
        tx_errors: 0
root@PicOS-OVS$
```

5 Reset one queue according to queue-uuid

```
root@PicOS-OVS$ovs-vsctl set queue f7c5e8ff-f81f-4e69-9096-9b1251f29618 other-config=min-rate=100000000,weight=2
root@PicOS-OVS$
root@PicOS-OVS$ovs-appctl qos/show te-1/1/3
QoS: te-1/1/3 PRONTO_WEIGHTED_ROUND_ROBIN
Default:
        burst: 0
        max-rate: 0
        min-rate: 100000000
        weight: 2
        tx_packets: 0
        tx_bytes: 0
        tx_errors: 0
Queue 3:
        burst: 0
        max-rate: 0
        min-rate: 200000000
        weight: 3
        tx_packets: 0
        tx_bytes: 0
        tx_errors: 0
root@PicOS-OVS$
```

6 Remove one queue from qos according qos-uuid and queue-key.

```
root@PicOS-OVS$ovs-vsctl remove qos b41dbaab-dc60-40ff-8a11-7a241bfd5a5c queue 3
root@PicOS-OVS$
root@PicOS-OVS$ovs-appctl qos/show te-1/1/3
QoS: te-1/1/3 PRONTO_WEIGHTED_ROUND_ROBIN
Default:
        burst: 0
        max-rate: 0
        min-rate: 100000000
        weight: 2
        tx_packets: 0
        tx_bytes: 0
        tx_errors: 0

root@PicOS-OVS$ovs-vsctl destroy queue 5d57cffb-b9b7-4324-9402-034ab9fac050
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list queue
_uuid               : f7c5e8ff-f81f-4e69-9096-9b1251f29618
dscp                : []
external_ids        : {}
```

```
other_config        : {min-rate="100000000", weight="2"}
```

7 Add one new queue to qos according qos-uuid

```
root@PicOS-OVS$ovs-vsctl set qos b41dbaab-dc60-40ff-8a11-7a241bfd5a5c queues:1=
@newqueue1 -- --id=@newqueue1 create queue other-config:weight=3
02273a2b-f556-454f-959f-96290dac7642
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list qos
_uuid               : b41dbaab-dc60-40ff-8a11-7a241bfd5a5c
external_ids        : {}
other_config        : {}
queues              : {0=f7c5e8ff-f81f-4e69-9096-9b1251f29618, 1=02273a2b-f556-454f-959f-96290dac7642}
type                : PRONTO_WEIGHTED_ROUND_ROBIN
```

8 Remove all queues from qos

```
root@PicOS-OVS$ovs-vsctl clear qos b41dbaab-dc60-40ff-8a11-7a241bfd5a5c queues
root@PicOS-OVS$ovs-vsctl --all destroy queue
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list queue
root@PicOS-OVS$
root@PicOS-OVS$ovs-appctl qos/show te-1/1/3
QoS: te-1/1/3 PRONTO_STRICT
root@PicOS-OVS$
```

9 Remove qos

```
root@PicOS-OVS$ovs-vsctl clear port te-1/1/3 qos
root@PicOS-OVS$ovs-vsctl --all destroy qos
root@PicOS-OVS$
```

WFQ

The full name of WFQ is Weighted Fair Queuing. It is similar to WRR. The only difference between WFQ and WRR is that the scheduling mode in WRR is by packets but in WFQ is by bytes.

Example

```
ovs-vsctl -- set port te-1/1/4 qos=@newqos -- --id=@newqos create qos type=PRONTO_WEIGHTED_FAIR_QUEUING queues:1=@
other-config=min-rate=300000000,weight=5  -- --id=@newqueue1 create queue other-config=min-rate=100000000,weight=5
```

CoS Mapping

In PicOS-2.1, if user enables the Class of Service (CoS) mapping, the packet will be mapped to a physical queue (0-7). With DSCP (0-7), it maps to queue-0 and with DSCP (8-16), it maps to queue-1 and so on. Queue-7 has the highest priority. Enable the CoS Mapping as follows:

```
admin@PicOS-OVS$ovs-vsctl set-cos-map true

admin@PicOS-OVS$ovs-vsctl show-cos-map
cos mapping: enabled
```

Display the configuration by entering the following:

```
admin@PicOS-OVS$ovs-vsctl show-cos-map ge-1/1/1
cos mapping: enabled
{
       dscp   queue
    --------  -----
     0 -  7:   q0
     8 - 15:   q1
    16 - 23:   q2
    24 - 31:   q3
    32 - 39:   q4
    40 - 47:   q5
    48 - 55:   q6
    56 - 63:   q7
}
```

To configure a flow, use the following command:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=set_queue:7,output=3
```

The action of "**set-queue:7**" will take the place of the default CoS mapping.

Modify the dscp value of port:

```
admin@XorPlus$ovs-vsctl set-cos-map true
admin@XorPlus$
admin@XorPlus$ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2
admin@XorPlus$ovs-vsctl show-cos-map ge-1/1/1
cos mapping: enabled
{
dscp queue
-------- -----
0: q1
1: q1
2: q2
others: q0
}
admin@XorPlus$
```

The following command is also permitted:

```
admin@XorPlus$ovs-vsctl set interface ge-1/1/2 dscp_map:0=q1 dscp_map:1=q1 dscp_map:2=q2
admin@XorPlus$
admin@XorPlus$
admin@XorPlus$ovs-vsctl show-cos-map ge-1/1/2
cos mapping: enabled
{
dscp queue
-------- -----
0: q1
1: q1
2: q2
```

```
others: q0
}
admin@XorPlus$
```

WRED

WRED

WRED(short for Weighted Random Early Detection) is a congestion avoidance mechanism which makes use of the congestion control mechanism of TCP (Transmission Control Protocol). When an output queue begins to experience congestion, WRED starts dropping packets *selectively.*By dropping some packets earlier than the point when the queue is full, WRED prevents the situation where a large number of packets get dropped at once. The principle specifys as follows:

(1)The length of the queue(measured with kbps or pktps) is calculated.

(2)If the queue length is less than the minimum threshold, the packet is placed in the queue.

(3)If the queue length is more than the maximum threshold, the packet is dropped.

(4)If the queue length is more than the minimum threshold but less than the maximum threshold, the packet is either dropped or queued, based on the packet drop probability. The greater the chance of the packet is dropped when the drop_probability value of its corresponding queue is greater.Usually,the drop_probability value of the lower priority queues with less importance are the greatest.

1 Create two wred_queues for interface te-1/1/35

```
root@PicOS-OVS$ovs-vsctl set interface te-1/1/35 wred_queues:0=@wred1 wred_queues:3=@wred2 -- --id=@wred1 create wred_queue enable=true
52f26264-3656-4840-8f0e-fb7be8e52ef8
9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=34,dl_src=22:11:11:11:11:11,actio
ns=set_queue:3,output=35
```

Notice: The drop_probability is according to the percentage to drop packets.

2 Check wred queues

```
Check all wred_queue:
root@PicOS-OVS$ovs-vsctl list wred_queue
_uuid               : 52f26264-3656-4840-8f0e-fb7be8e52ef8
drop_probability    : 50
enable              : true
max_thresh          : 200
min_thresh          : 100
_uuid               : 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
drop_probability    : 40
enable              : true
max_thresh          : 400
min_thresh          : 200
root@PicOS-OVS$

Check one wred_queue:
root@PicOS-OVS$ovs-vsctl list wred_queue 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
_uuid               : 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
drop_probability    : 40
enable              : true
max_thresh          : 400
min_thresh          : 200
root@PicOS-OVS$

Check interface wred_queue:
root@PicOS-OVS$ovs-vsctl list interface te-1/1/35
_uuid               : db795f1d-71e9-448c-9ac4-f2304c4bf74d
............
............
status              : {}
type                : "pica8"
wred_queues         : {0=f37f30cf-8470-4edd-925f-5c2abcd061eb, 3=b97fa496-57b2-40f1-a525-b978abc64403}
root@PicOS-OVS$
```

3 Reset one wred queue according to its uuid

```
root@PicOS-OVS$ovs-vsctl set wred_queue 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d max_thresh=300

root@PicOS-OVS$ovs-vsctl list wred_queue 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
_uuid               : 9b36b9dc-903a-4bb6-8e25-f6e2b1fd2b4d
drop_probability    : 40
enable              : true
max_thresh          : 300
min_thresh          : 200
root@PicOS-OVS$
```

4 Add one wred queue to wred_queues

```
root@PicOS-OVS$ovs-vsctl set interface te-1/1/35 wred_queue:1=@wrednew -- --id=@wrednew create wred_queue enable=true min_thresh=100 ma
d60801bd-827b-45b7-aa5d-1a2db9f1e513
root@PicOS-OVS$
```

5 Remove one or all wred queue

```
Remove one wred queue:
root@PicOS-OVS$ovs-vsctl remove interface te-1/1/35 wred_queues 3
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list wred_queue
_uuid               : 52f26264-3656-4840-8f0e-fb7be8e52ef8
drop_probability    : 50
enable              : true
max_thresh          : 200
min_thresh          : 100
_uuid               : d60801bd-827b-45b7-aa5d-1a2db9f1e513
drop_probability    : 40
enable              : true
max_thresh          : 500
min_thresh          : 100
root@PicOS-OVS$

Delete all wred queues:
root@PicOS-OVS$ovs-vsctl clear interface te-1/1/35 wred_queues
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl list wred_queue
root@PicOS-OVS$
```

WRED-ECN

From PicOS2.10.0, pica8 switch support enable ecn.

ECN (short for Explicit Congestion Notification)is a property of queue. When congestion occurs, WRED drops packets based on the queue length exceeding certain threshold value.But if you enable ECN on a queue,the packets are marked instead of dropped. Downstream routers and hosts would see this marking as an indication of network congestion and slow down their packet transmission rates.

ECN is a value in the DS (Differentiated Services) field of the IPv4 protocol header. ECN uses the two least significant (right-most) bits of the 8-bit DF field to encode four different codepoints:

(1)00 - Not ECN-Support Transport

(2)01 - ECN-Support Transport(1)

(3)10 - ECN-Support Transport(0)

(4)11 - Congestion Experienced

When both end hosts support ECN they mark their packets with either 10 or 01. When WRED and ECN is enabled and the queue is congested, the PicOS changes the ECN field of all such packets to 11. When ECN is not enabled, the ECN bits are not changed.

> 1, WRED-ECN only support in unicast flow entry.

Command:

ECN take effect when enabling WRED on a port.The ecn value of each queue can be different,you can use command like this, disable ecn in queue2 and enable ecn in queue5.

```
ovs-vsctl set-port-wred-ecn ge-1/1/1 2=false 5=true
```

If user want to make the ecn values of all queues are equal,you can use command like this for simplification.

```
ovs-vsctl set-port-wred-ecn ge-1/1/1 true/false
```

Show wred-ecn

```
ovs-vsctl show-port-wred-ecn ge-1/1/1
```

Example:

1, Add bridge ports and configure wred in physical port te-1/1/4 queue0.

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1 -- set interface te-1/1/2 options:link_speed=1G
ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1 -- set interface te-1/1/3 options:link_speed=1G
ovs-vsctl add-port br0 te-1/1/4 vlan_mode=trunk tag=1 -- set interface te-1/1/4 options:link_speed=1G

ovs-vsctl set interface te-1/1/4 wred_queues:0=@wred1 -- --id=@wred1 create wred_queue enable=true min_thresh=100 max_thresh=200 drop_p
```

2, enable ecn in port te-1/1/4.

```
ovs-vsctl set-port-wred-ecn te-1/1/4 true
ovs-vsctl show-port-wred-ecn te-1/1/4
```

3, add unicast flow entry.

```
ovs-ofctl add-flow br0 in_port=2,dl_dst=22:00:00:00:00:11,dl_vlan=1,ip,actions=push_mpls:0x8847,set_field:10-\>mpls_label,set_queue:0,output:4
ovs-ofctl add-flow br0 in_port=3,dl_dst=22:00:00:00:00:22,dl_vlan=1,ip,actions=push_mpls:0x8847,set_field:20-\>mpls_label,set_queue:0,output:4
ovs-appctl pica/dump-flows
```

Vlan Priority CoS Mapping

From PicOS-2.11, the vlan priority cos mapping is disabled default, user can enable it and configure special mapping in ingress interface. Enable vlan priority cos mapping will make the ingress packes which with different vlan_pcp enter different queues.

> 1, Before PicOS-2.11, the vlan priority cos mapping is enabled defaultly, and cannot configure the mapping.
>
> 2, If enable ***vlan-priority-cos-map*** and traffic can match the flow 'in_port=1,actions=output:2' in switch, the original traffic will send out from switch; if disable ***vlan-priority-cos-map,*** the traffic no mater attach which vlan_pcp will be change the vlan_pcp to 0 and send out from switch.
>
> 3, If enable ***vlan-priority-cos-map*** and ***cos-map*** , and traffic can match both of the mapping at same time, at last the cos-mapping working.

Command:

1, Check vlan priority cos mapping state:

ovs-vsctl show-vlan-priority-cos-map

2, Enable/disable vlan priority cos mapping:

ovs-vsctl set-vlan-priority-cos-map TRUE|FALSE

3, Once enable the mapping, user can see the default mapping is vlan_pcp 0~7 mapping queue 0~7.

ovs-vsctl show-vlan-priority-cos-map <interface>

4, configure the mapping:

ovs-vsctl set interface <interface> vlan_priority_mapping=<vlan_pcp>=q<queue number>[,<vlan_pcp>=q<queue number>,...]

5, user also can configure the untag packet same as one vlan_pcp and send to the mapping queue:

ovs-vsctl set interface <interface> vlan_priority_untagged=<vlan_pcp>

Example:

1, enable vlan-priority-cos-map, and show the mapping in interface te-1/1/9

```
admin@PICOS-OVS$ovs-vsctl set-vlan-priority-cos-map TRUE
admin@PICOS-OVS$ovs-vsctl show-vlan-priority-cos-map
vlan priority cos mapping: enabled

admin@PICOS-OVS$ovs-vsctl show-vlan-priority-cos-map te-1/1/9
vlan priority cos mapping: enabled
{
    vlan-priority   queue
    -------------  -------
               0    q0
               1    q1
               2    q2
               3    q3
               4    q4
               5    q5
               6    q6
               7    q7
}
```

2, configure the mapping, vlan_pcp:7 enter queue3, vlan_pcp:6 enter queue2, and others enter default queue0.

```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/9 vlan_priority_mapping=7=q3,6=q2
admin@PICOS-OVS$
admin@PICOS-OVS$ovs-vsctl show-vlan-priority-cos-map te-1/1/9
vlan priority cos mapping: enabled
{
    vlan-priority   queue
    -------------  -------
               6:   q2
               7:   q3
         others:   q0
```

```
}
```

3, set untag packets same as vlan_pcp:7 and enter queue3.

```
admin@PICOS-OVS$ovs-vsctl set interface te-1/1/9 vlan_priority_untagged=7
```

4, add flow entry, in_port is port te-1/1/9, the untag packets which enter from port te-1/1/9 will be send to queue3.

```
admin@PICOS-OVS$ovs-ofctl add-flow br0 in_port=9,actions=output:10
```

Configuring Flow Table

Combinated Mode

Our switches support such a command "*ovs-vsctl set-combinated-mode true | false".*This command is for resolving the packets forwarding problem of push_vlan. Sometimes,the packets forwarding is not as expected.

Eg：there are two flows in our switch below:

priority=100, in_port=1, dl_vlan=1, actions=push_vlan:100, output:2

priority=110,in_port=1,dl_vlan=100,actions=output:3

Sending packets match to the first flow: We expect the packets to forward to port 2 after pushing vlan 100, but the actual result is that port 3 receives these packets with outer vlan 100.

In order to solve this kind of problem, we add a new command "ovs-vsctl set-combinated-mode true|false". When enabling this combinated mode, each flow can have a new match field class-id added. Each flow has a different class-id, so the packets can be forwarded correctly. In hardware,each flow is separated with two flows with class-id as following:

When user adds such two flows to the switch:

priority=100, in_port=1, dl_vlan=1, actions=push_vlan:100, output:2

priority=110,in_port=1,dl_vlan=100,actions=output:3

In hardware,this flow can be sepeared to two parts in icap and vcap:

vcap: priority=100, class-id=1, in_port=1, dl_vlan=1, and push_vlan 100

icap: priority=100, class-id=1, in_port=1, dl_vlan=100, and output:2

priority=110, class-id=2, in_port=1, dl_vlan=100, and output:3

Commands

enable combinatedmode

```
admin@PicOS-OVS$ovs-vsctl set-combinated-mode true
```

disable combinated mode(by default)

```
admin@PicOS-OVS$ovs-vsctl set-combinated-mode false
```

Example

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set interface ge-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set interface ge-1/1/2 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set interface ge-1/1/3 type=pica8
admin@PicOS-OVS$ovs-vsctl set-combinated-mode true
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=100,in_port=1,dl_vlan=1,actions=push_vlan:100,output:2
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=110,in_port=1,dl_vlan=100,actions=output:3
```

When sending packets match the first flow with dl_vlan=1 to ge-1/1/1,then ge-1/1/2 will forward packets with outer vlan 100, not ge-1/1/3. This will provide our expected result.

Note

1. When enabling or disabling combinated mode, all the flows in table 0 are evicted from the switch, except the default **drop** flow;

2.When enabling combinated mode, the max flow numbers including push_vlan and other normal flows is different in different platforms:

P5401&&P5101&&P3922&&P3930&&AS6701&&P3780: the max number is 512.

P3290&&P3297&&P3295:the max number is 1024

Configuring ECMP

Command

ovs-vsctl set-max-ecmp-ports *[numbers]*

ovs-vsctl show-max-ecmp-ports

Parameters

Numbers:[2-32],max is 32 ,and this must be 2^n(n=1,2,3,4,5). ***Default*** *number is 4.*

Example

PicOS OVS supports ecmp (nw_src, nw_dst),the default ecmp ports is 4.
IP packets (nw_src=192.168.1.0/255.255.255.1) will forward to port 2.
IP packets (nw_src=192.168.1.1/255.255.255.1) will forward to port 3.

```
root@PicOS-OVS#ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:2,bucket=output:3
root@PicOS-OVS#ovs-ofctl add-flow br0 dl_type=0x0800,nw_src=192.168.1.0/24,actions=group:1
```

If port 2 is down, all packets will forward to port 3.

Configuring egress flow table

In egress table,can not match mpls label in match field because the mpls label achived by udf and egress table are not achieved by udf.Supporting match fields are dl_type,vlan_tci,dl_dst,dl_src,src ip,dst ip,.tp_dst,tp_src.From version 2.10,pica8 switch support match "output_port" in egress table.The prerequisites using this match field is that must exist a flow with an output port in other flow table.

Egress mode is disabled by default,users can enable this mode by command ***"ovs-vsctl set-egress-mode true [table_id]"***.The default table id is 253.

Command

ovs-vsctl set-egress-mode true [table_id]

table_id range is 0~254.default value is 253.

Egress Flow

The flows' match field must include table_id,the actions of egress flow can be ***drop,mod_nw_tos,set_queue***.When you want to modify the tos value,***dl_type*** is neccessary in match field.

eg:

```
ovs-vsctl set-egress-mode true
ovs-ofctl add-flow br0 table=253,in_port=1,ip,actions=mod_nw_tos:32
```

Example

add a flow in icap table

```
ovs-ofctl add-flow br0 in_port=2,dl_vlan=10,actions=set_field:20-\>vlan-vid,3
```

enable egress mode

```
ovs-vsctl set-egress-mode true
```

add a flow to table 253

```
ovs-ofctl add-flow br0 table=253,in_port=2,output_port=3,dl_vlan=20,actions=drop
```

Configuring Flow Handling Mode

PicOS supports set-flow-handling-mode from version 2.7.1. If the flow is integrated and can be installed directly, there is no need for set-flow-handling-mode, and whatever mode it is, it should be installed. But If the hardware does not support the actions, or the flow is not an exact match, it will not be installed directly. This is where we need set-flow-handling-mode, to decide what to do with the flow, whether to install the flow and how to install it.

The command is:

```
admin@PicOS-OVS$ovs-vsctl set-flow-handling-mode [mode]
```

Mode value: [enable_packet_driven, hardware_flow_only, software_flow_allowed], and default value is software_flow_allowed.

After setting a particular flow handling mode, the switch should be rebooted to make the mode effective.

```
admin@PicOS-OVS$ovs-vsctl show-flow-handling-mode
```

Direct Flows

These flows can be installed directly to the hardware table whatever mode it is.

Example 1

```
admin@XorPlus$ovs-ofctl add-flow br0 in_port=9,ip,actions=push_vlan:0x8100,set_field:19-\>vlan_vid,output:11
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#96 normal permanent flow_id=18 ip,in_port=9, actions:push_vlan(vid=19),mod_vlan_pcp(pcp=0),11
normal_d permanent internal flow_id=7 priority=0, actions:drop
Total 1 flows in HW.
admin@PicOS-OVS$
```

Example 2

```
admin@XorPlus$ovs-ofctl add-flow br0 in_port=9,dl_vlan=19,dl_dst=22:22:22:22:22:22,tcp,actions=set_field:3.3.3.3-\>
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
normal_d permanent internal flow_id=7 priority=0, actions:drop
#98 normal permanent flow_id=20 tcp,in_port=9,dl_vlan=19,dl_dst=22:22:22:22:22:22, actions:set(ipv4(dst=3.3.3.3)),s
Total 1 flows in HW.
admin@PicOS-OVS$
```

Regardless of whatever flow handling mode is currently in effect, direct flows will always be installed to the hardware table directly.

Packet-driven-flows

The packet-driven status is as follows:

set-flow-handling-mode = hardware_flow_only

This mode forbids the flow installation if the hardware does not support the actions or the flow is not an exact match.

Example

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=9,tcp,dl_vlan=19,actions=set_field:192.168.1.1-\>nw_src,set_field:0x
OFPT_ERROR (OF1.4) (xid=0x2): OFPBAC_MATCH_INCONSISTENT
OFPT_FLOW_MOD (OF1.4) (xid=0x2):
(***truncated to 64 bytes from 136***)
00000000  05 0e 00 88 00 00 00 02-00 00 00 00 00 00 00 00 |................|
00000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 80 00 |................|
00000020  ff ff ff ff ff ff ff ff-ff ff ff ff 00 00 00 00 |................|
00000030  00 01 00 1d 80 00 00 04-00 00 00 09 80 00 0a 02 |................|
admin@PicOS-OVS$
```

In hardware_flow_only mode, configuring packet-driven flows will return an error.

set-flow-handling-mode = software_flow_allowed

This mode forbids the flow installation if the hardware does not support the actions. This mode permits the flow installation TO_CPU if the hardware supports the action but the flow is not exact an match. The item will be submitted to the CPU for further actions .

Example

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=9,ip,dl_vlan=199,actions=push_mpls:0x8847,set_field:299-\>mpls_label
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#1 normal_d permanent flow_id=12 priority=0, actions:drop
#2 normal_u permanent flow_id=16 ip,in_port=9,dl_vlan=199, actions:To_CPU(for_packet_driven)
Total 2 flows in HW.
admin@PicOS-OVS$
```

Packets which match this flow will be submitted to cpu, and it will not be forwarded at line-speed.

set-packet-driven-mode = enable_packet_driven

This mode forbids the flow installation if the hardware does not support the actions. This mode permits the flow installation TO_CPU if the hardware supports the actions but the flow is not an exact match. The item will be submitted to the CPU. The CPU will modify the match and make it exact by parsing, then install the exact flow.

Example

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=9,dl_dst=22:22:22:22:22:22,udp,actions=set_field:192.168.100.2-\>nw_
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#1 normal_d permanent flow_id=12 priority=0, actions:drop
#3 normal_u permanent flow_id=17 udp,in_port=9,dl_dst=22:22:22:22:22:22, actions:To_CPU(for_packet_driven)
Total 2 flows in HW.
admin@PicOS-OVS$
```

The packets matching this flow are checked in the hardware table, if there is no exact match, the packets are forwarded to the CPU. The CPU will modify the match and install the exact match flow on to the hardware table.

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#2 normal flow_id=11 priority=1048560,udp,in_port=9,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:22,nw_dst=2.2.2.2
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#1 normal_u permanent flow_id=11 udp,in_port=9,dl_dst=22:22:22:22:22:22, actions:To_CPU(for_packet_driven)
Total 3 flows in HW.
admin@PicOS-OVS$
```

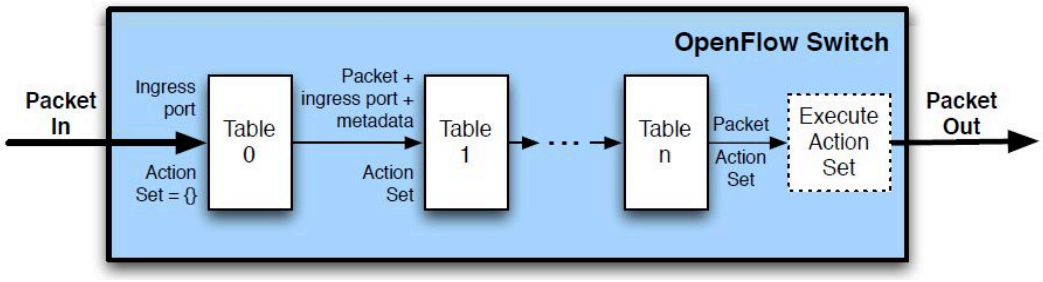
Packets can then be transmitted at line-speed since there is now an exact match flow entry in the hardware table.

> ⚠ In case of direct flows, the set-packet-driven-mode is irrelevant and can be ignored. It is only when the flows cannot be installed directly, that the set-packet-driven-mode becomes necessary. The underlying hardware support is crucial to adding flows, if there is no support for the flow in the hardware, the system will generate an error message.

Configuring Multi-Table

Hardware OpenFlow Multi-table Limitations

OpenFlow 1.1 and later versions have a concept of tables--independent lookup tables that can be chained in any way user wishes. This is a very useful concept to decrease the number of flows by segmenting those flows in multiple tables.



The implementation of those multiple tables is not difficult in a software based switch like OVS, but it is a substantial issue for a hardware based switch. This is because most ASIC's have a limited set of capacities and the ability to do multiple lookup on packets is severely limited.

The multi-table concept is very useful though to emulate an ASIC Pipeline. It allows the Openflow based solution to leverage a lot more of the Switch ASIC capacities like complex lookup or different types of memory available on the ASIC. A hardware based multi-table implementation must be limited to reflect the limitation of the underlying ASIC.

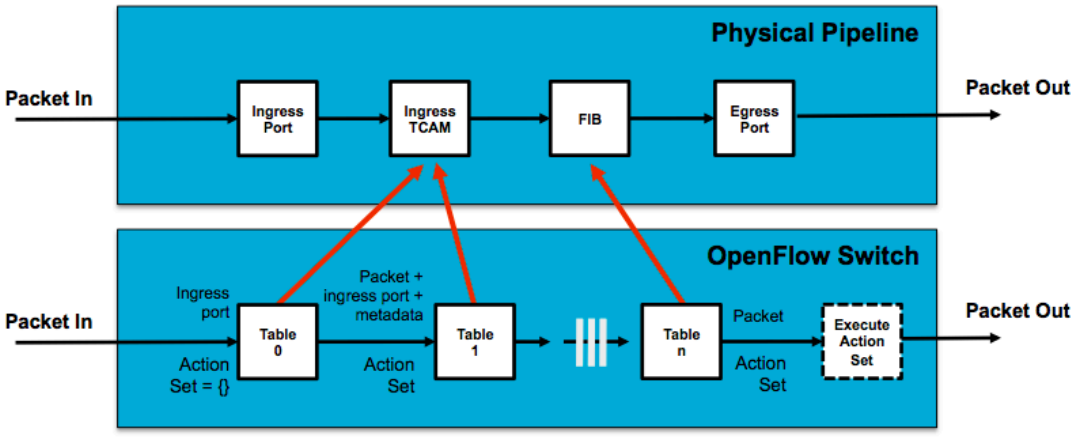
This means that the number of tables, the conflict between tables, the capacity of those tables and the link between them will be limited by the implementation. This is now defined more generically as a Table Typed Patterned by the ONF.

Multi-Tables in TCAM

Traditionally in a hardware based Openflow implementation, the flows are placed in the switch TCAM memory. This is because this memory is perfect for complex matching (can match on many parts of the packet header and the actions possible once the flow is matched are very diverse) and as such is a good match for most Openflow solutions.

In PicOS, by default, all Openflow tables are implemented in TCAM.

It is possible to create multiple tables, but because only one table is available, the OS is normalizing the flows into only one hardware table (table 0).



(a) Packetes are matched against multiple tables in the pipeline

Because the normalizing process cannot simulate all the types of multi table logic, using this TCAM-only Multi-table implementation is typically not recommended. It is mainly used as a proof of concept or demonstration purpose.

One way to be sure that the normalizing process will render the logic of the flows correctly, is to have only one of the tables with actions. All the other tables should only have drop or goto action.

Note:

- If adding L2/L3 flow entry applied to one port which does not exist in the bridge, the flow cannot add correctly.
- Command of adding L3 flow modified. User must enable L2 mode first and add a system mac flow (the action is normal in ovs2.3, the actions is goto_l3 in ovs2.6) to the L2 table. If user wants to use the L3 table to do the routing.
- The route flows are limited to 12000 by default.

Using the Forwarding Database instead of the TCAM

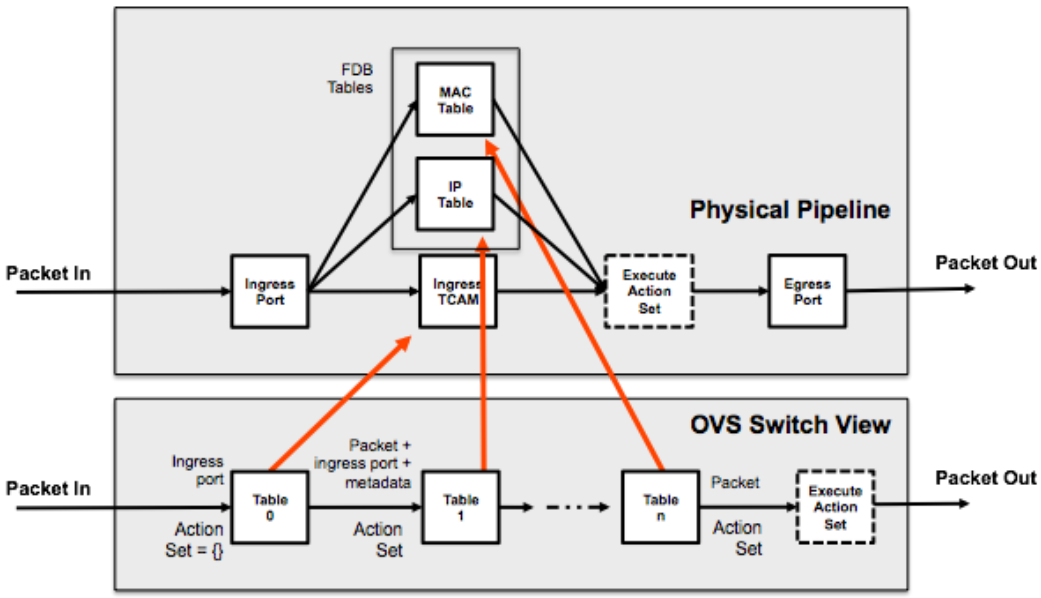
Starting in version 2.4, PicOS supports the FDB (forwarding database) table or ROUTE table like the traditional L2/L3 mode. That is to say the flows can be stored not only in TCAM table but also in FDB or ROUTE table. See the Switch Hardware Architecture for a description of the actual hardware pipeline.

This is very useful when the scaling of the solution is important and this allows the usage of more memories on the switch, as well as access to a more complex lookup.

The FDB tables consist of a MAC table (similar to a typical L2 Switch Mac lookup) and an IP Table (similar to a typical L3 Router IP lookup). User can select to download flows into the TCAM (default), the MAC table, or the IP table.

Every packet will match all those tables. Conflict between tables (different action in different tables) is managed by the table priority which can be configured.

OpenFlow "goto" action is not supported between tables. In this hardware implementation, all tables will be used.



To Map a specific OpenFlow table to the MAC table, use the command:

set-l2-mode TRUE|FALSE [TABLE] command to *enable the MAC table to store flows.* ***[TABLE]*** is the table number which table user set as the FDB table. By default it is the table 251. The flow in the TCAM table should strictly match dl_dst,dl_vlan, (output port in action of flow).

To Map a specific OpenFlow table to the IP table, use the command:

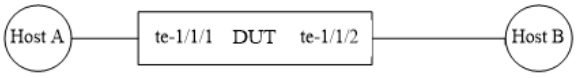
set-l3-mode TRUE|FALSE [TABLE] command to *enable the ROUTE table to store flows.* ***[TABLE]*** is the table number user set as the ROUTE table. By default, the ROUTE table number is 252. The flows to be stored in ROUTE must strictly match dl_type,nw_dst, (mod_dl_dst,mod_dl_vlan,output port in action of flow). But user should add a flow with normal action to FDB table first if user wants the L3 flow to work.

By default, TCAM matching has higher priority than L2/L3, and the priority is 0. User can use the command '**ovs-vsctl set-l2-l3-preference true**' to have the FIB/MAC table with a higher priority than the TCAM table.

By default, the ROUTE table is higher priority than the MAC table.

It is possible to have a maximum of 3 hardware tables with flows in our current implementation simultaneously: 1 TCAM table, 1 ROUTE table and 1 MAC table.

Examples



FDB table configuration example

Step 1: Create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

Step 3: Set L2-mode true without table number

```
admin@PicOS-OVS$ovs-vsctl set-l2-mode true
```

Step 4: Add a flow with table = 251

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=251,dl_vlan=10,dl_dst=22:22:22:22:22:22,actions=output:2
```

Check the flows in hardware using command ***ovs-appctl pica/dump-flows.*** User will see that the flow is stored in L2 table. If user wants table 2 to be the FDB table, use the ***ovs-vsctl set-l2-mode true 2*** command.

ROUTE table configuration example

Step 1: Create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

Step 3: Set L3-mode true without table number

```
admin@PicOS-OVS$ovs-vsctl set-l3-mode true
```

Step 4: Add a flow with table = 252

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=251,dl_dst=22:22:22:22:22:22,dl_vlan=10,actions=normal
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=252,dl_type=0x0800,nw_dst=192.168.2.30,actions=set_field:44:44:44:22:
```

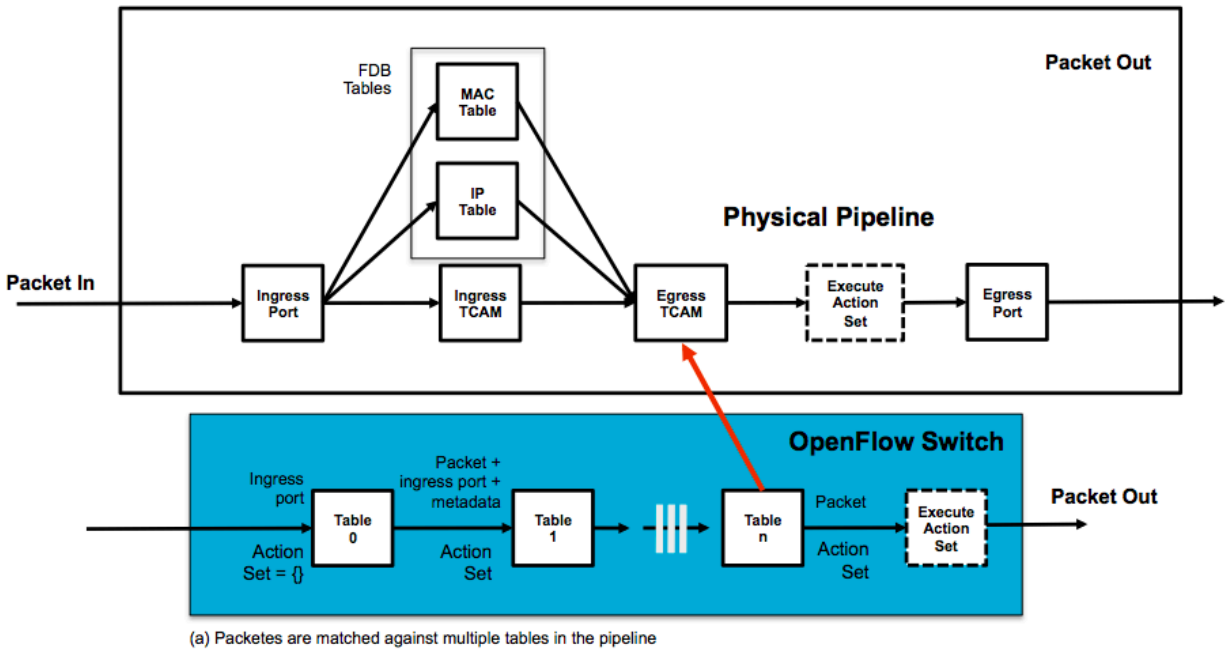
Check the flows in hardware using command ***ovs-appctl pica/dump-flows.*** User will see that the flow is stored in L3 table. If user wants table 4 to be the FDB table, use the ***ovs-vsctl set-l3-mode true 4*** command.

Egress Flow Table

The match in the egress openflow table is very similar to the ingress tcam table. Only some ipv6 fields cannot be matched.
The full match list is in_port, src_mac, dst_mac, ether_type, vlan_id, vlan_priority, ip_protocol, ipv4_src_addr, ipv4_dst_addr, ipv4_tos, tcpudp_src_port, tcpudp_dst_port.

The size of egress table is 512 flows for most platforms (one exception is the P-3290 limited to only 256 flows).

For a full description of the command usage to configure the egress TCAM, see: Egress-mode Command



(a) Packetes are matched against multiple tables in the pipeline

- Multitable Resources

Multitable Resources

Description

From PicOS version 2.7.1, some new modifications have been made to the multitable feature with the addition of the "resource" feature. Different platforms have different resources.

(All platforms which support l2-l3-buffer-mode are as follows: as5712_54x, as6701_32x, as6712_32x, dcs7032q28, es4654bf, niagara2632xl, niagara2948_6xl, pronto5101, pronto5401, as4610_54p, as4610_54t, as4610_30p, as4610_30t)

Platforms	Buffer-mode Resources
as5712_54x	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000 "; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
as6701_32x	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000 "; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
as6712_32x	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000 "; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
dcs7032q28	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000"; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
es4654bf	"0" "l2-size 131072, host-route 13100, route 4800"; "1" "l2-size 98304, host-route 39300, route 4800"; "2" "l2-size 98304, host-route 13100, route 4800"; "3" "l2-size 32768, host-route 91700, route 4800"; "4" "l2-size 32768, host-route 13100, route 4800"; "5" "l2-size 32768, host-route 13100, route 4800";
niagara2632xl	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000"; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";

niagara2948_6xl	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000 "; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
pronto5101	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000 "; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
pronto5401	"0" "l2-size 294912, host-route 12000, route 12000"; "1" "l2-size 229376, host-route 44800, route 12000"; "2" "l2-size 163840, host-route 70400, route 12000"; "3" "l2-size 98304, host-route 96000, route 12000"; "4" "l2-size 32768, host-route 12000, route 115200"; "5" "l2-size 32768, host-route 12000, route 12000";
as4610_54p, as4610_54t, as4610_30p, as4610_30t	"0" "l2-size 65536, host-route 8192, route 6000"; "1" : "l2-size 49152, host-route 16384, route 6000"; "2" "l2-size 49152, host-route 24576, route 6000"; "3" "l2-size 49152, host-route 8192, route 6000"; "4" "l2-size 32768, host-route 24576, route 6000"; "5" "l2-size 32768, host-route 16384, route 6000";
Others (not support buffer mode)	"l2-size 32768, host-route 12000, route 12000";

First, user should enable the L2 and L3 mode. Then, use the command "**ovs-appctl pica/show tables "** to check the L2 and L3 max flows in the switch.

Example

Step 1: Add bridge and port

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 te-1/1/77 vlan_mode=trunk tag=1 -- set Interface te-1/1/77 type=pica8
ovs-vsctl add-port br0 te-1/1/78 vlan_mode=trunk tag=1 -- set Interface te-1/1/78 type=pica8
```

Step 2: Enable L2 and L3 mode

```
ovs-vsctl set-l2-mode true
ovs-vsctl set-l3-mode true
```

Step 3: Check the default resources

```
admin@PicOS-OVS$ovs-appctl pica/show tables
Pica Tables Statistics:
    Pica Tables              Max Limitation          Current Used
    ------------------------------------------------------------------------
    ICAP Table                 2044                    10
    ECAP Table                 (null)                  (null)
    VCAP Table                 512                     0
    L2 System Table            512                     0
    L2 FDB Table               32256                   0
    L3 Host Table              12000                   IPv4(0),IPv6(0*2)
```

```
    L3 Route Table             12000                  IPv4(0),IPv6(0*2)
UDF Table                  (null)                 (null)
```

Step 4: Add L2 flows

```
ssun@dev-42:~/ryu/ryu/app$ ryu-manager simple_switch_13_ssun_buffer_mode5.py
 for i in range(4797, 5195):
             for k in ('0','1','2','3','4','5','6','7','8','9'):
                 for z in ('0','1','2','3','4','5','6','7','8','9'):
                     dl_dst="22:22:22:22:"+k+z+":22"
                     match=self.set_match(datapath, dl_dst=dl_dst, vlan_vid=i)
                     output_port=78
                     actions=self.set_action(datapath, out_port=output_port)
                     self.add_flow(datapath, 251, 32768, match, actions)
```

Step 5: Check max L2 flow members

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0|grep -c "table=251"
32256
admin@PicOS-OVS$ovs-appctl pica/show tables
Pica Tables Statistics:
    Pica Tables              Max Limitation          Current Used
    ------------------------------------------------------------------------
    ICAP Table                 2044                   8
    ECAP Table                 (null)                 (null)
    VCAP Table                 512                    0
    L2 System Table            512                    0
    L2 FDB Table               32256                  32256
    L3 Host Table              12000                  IPv4(0),IPv6(0*2)
    L3 Route Table             12000                  IPv4(0),IPv6(0*2)
UDF Table                  (null)                 (null)
```

Step 6: Delete L2 flows and add ipv4 net route (ipv4 l3 host ,ipv6 host ,ipv6 route)

```
admin@PicOS-OVS$ovs-ofctl del-flows br0
ssun@dev-42:~/ryu/ryu/app$ ryu-manager simple_switch_13_ssun_buffer_mode5.py
for j in range(0,51):
             for i in range(0,255):
                 output_port=78
                 tmp1='%d' %i
                 tmp2 = '%d' %j
                 ipv4_dst='192.168.' + tmp2 +' .' +tmp1
                 dl_dst="22:22:22:22:22:22"
                 vlan_vid=20
                 match=self.set_match(datapath, dl_type=0x0800, ipv4_dst=ipv4_dst, ipv4_dst_mask="255.255.255.255")
                 actions=self.set_action(datapath, dl_dst="44:44:44:88:88:88", vlan_vid=vlan_vid, out_port=output_p
                 self.add_flow(datapath, 252, 32768, match, actions)
```

Step 7: Check max ipv4 l3 flow members

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0|grep -c "table=252"
12000
admin@PicOS-OVS$ovs-appctl pica/show tables
Pica Tables Statistics:
    Pica Tables              Max Limitation          Current Used
    ------------------------------------------------------------------------
    ICAP Table                 2044                   10
    ECAP Table                 (null)                 (null)
    VCAP Table                 512                    0
    L2 System Table            512                    1
    L2 FDB Table               32256                  0
    L3 Host Table              12000                  IPv4(0),IPv6(0*2)
    L3 Route Table             12000                  IPv4(12000),IPv6(0*2)
UDF Table                  (null)                 (null)
```

Configuring NAT flow

The Network Address Translation (NAT) process maps IP addresses from one address domain (or realm) to another to provide transparent routing to end hosts. Typically, NAT allows organizations to map public external addresses to private or unregistered addresses. A flow with NAT actions (changing IP address or L4 port) can be hardware switched. Flows can be associated with the following actions: mod_nw_dst, mod_nw_src, mod_tp_dst and mod_tp_src.

Listed below is the minimal information needed to process the packet on hardware only (direct flow):

1) dl_dst(match field or action), dl_vlan(match field or action), mod_nw_src, mod_tp_src

2) dl_dst(match field or action), dl_vlan(match field or action), mod_nw_dst, mod_tp_dst

3) dl_dst(match field or action), dl_vlan(match field or action), tp_src(with or wthout in match field),mod_nw_src

4) dl_dst(match field or action), dl_vlan(match field or action), nw_src(match field),mod_tp_src

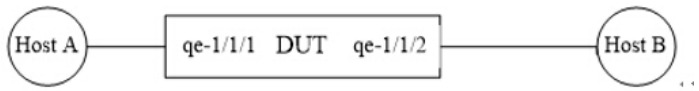
5) dl_dst(match field or action), dl_vlan(match field or action), tp_dst(with or wthout in match field),mod_nw_dst

6) dl_dst(match field or action), dl_vlan(match field or action), nw_dst(match field),mod_tp_dst

Supported Platform

Vendor	Platform
Delta	AG5648 v1-R, AG7648, AG9032v1
Accton	AS5712-54X, AS5812-54T, AS5812-54X, AS5835-54T, AS5835-54X, AS6712-32X, AS6812-32X, AS7312-54X, AS7326-56X, AS7712-32X, AS7726-32X, AS7816-64X
Dell	N3248X-ON, N3248PXE-ON, S4048-ON, S4128T-ON, S4128F-ON, S4148T-ON, S4148F-ON, S5212F-ON, S5224F-ON, S5248F-ON, S5232F-ON, S5296F-ON, Z9100-ON, Z9264F-ON
FS	N8560-32C, N8560-64C

Example



Example 1: SNAT

Step 1: Create a new bridge named br0.

```
admin@PicOS-OVS$ovs-vsctl add-br br0  -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1-- set interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1-- set interface te-1/1/2 type=pica8
```

Step 3: If user is inside network and wants to visit outside network, source IP needs to be modified:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,tcp,dl_vlan=1999,dl_dst=22:22:22:22:22:22,actions=set_field:192.1(
```

Step 4: Check flow tables.

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=264.202s, table=0, n_packets=n/a, n_bytes=0, tcp,in_port=1,dl_vlan=1999dl_dst=22:22:22:22:22
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#7417 normal permanent recirc_id=0,tcp,in_port=1,dl_vlan=1999,dl_dst=22:22:22:22:22:22,actions:set(ipv4(src=192.168
#7416 normal permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
```

```
admin@PicOS-OVS$
```

Example 2: DNAT

Step 1: Create a new bridge named br0

```
admin@PicOS-OVS$ovs-vsctl add-br br0  -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1-- set interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1-- set interface te-1/1/2 type=pica8
```

Step 3: If user is outside network and wants to visit inside network, destination IP needs to be modified:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,tcp,dl_vlan=1999,dl_dst=22:22:22:22:22:22,actions=set_field:192.1
```

Step 4: Check flow tables

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=264.202s, table=0, n_packets=n/a, n_bytes=0, tcp,in_port=1,dl_vlan=1999,dl_dst=22:22:22:22:22
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#7417 normal permanent recirc_id=0,tcp,in_port=1,dl_vlan=1999,dl_dst=22:22:22:22:22:22,actions:set(ipv4(dst=192.168
#7416 normal permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
admin@PicOS-OVS$
```

Example 3: Packet-driven-flow

If match field or actions cannot satisfy condition of direct flow, this flow will be packet-driven-flow, and it cannot be added to hardware table directly.

Establish br0 and add ports in br0 like above configration. And add flow as follows:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,tcp,actions=set_field:192.168.5.5-\>nw_src,set_fie
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=3.442s, table=0, n_packets=n/a, n_bytes=0, tcp,in_port=1 actions=set_field:192.168.5.5->ip_s
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#7460 normal permanent recirc_id=0,tcp,in_port=1, actions:To_CPU(for_packet_driven)
#7458 normal permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
admin@PicOS-OVS$
```

Sending increasing dst_mac packets to te-1/1/1, mac address from 22:22:22:22:22:22 to 22:22:22:22:22:2b, then check tables:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=135.680s, table=0, n_packets=n/a, n_bytes=1124112312, tcp,in_port=1 actions=set_field:192.168
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#7479 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:22,nw_src=2.0
#7478 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:2a,nw_src=2.0
#7477 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:29,nw_src=2.0
#7475 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:27,nw_src=2.0
#7471 normal priority=1048560,recirc_id=0,tcp,in_port=1,nw_src=192.168.5.5,nw_frag=no,tp_src=1110, actions:2
#7476 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:28,nw_src=2.0
#7472 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=00:00:00:00:00:00,nw_src=2.0
#7484 normal permanent recirc_id=0,tcp,in_port=1, actions:To_CPU(for_packet_driven)
#7483 normal permanent priority=0,recirc_id=0, actions:drop
#7480 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:23,nw_src=2.0
#7482 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:26,nw_src=2.0
#7481 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:24,nw_src=2.0
#7474 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:2b,nw_src=2.0
#7473 normal priority=1048560,recirc_id=0,tcp,in_port=1,vlan_tci=0x0000/0x1fff,dl_dst=22:22:22:22:22:25,nw_src=2.0
```

```
Total 14 flows in HW.
admin@PicOS-OVS$
```

1. And te-1/1/2 receive packets with the src_ip 192.168.5.5 and src_port 1110.

Due to ASIC limitation, a flow can not modify l4_src_port without modifying SIP or modify l4_dst_port without modifying DIP.

If only modifying SIP(DIP) or SIP+L4_SRC_PORT(DIP+L4_DST_PORT), up to 2k flow can be configured. If modifying both SIP[|L4_SRC_PORT] and DIP[|L4_DST_PORT], the flow supported is 1k.

2. If set_dl_src is included in actions, the packets will be stamped with set_dl_src (as before). If set_dl_src is not included in actions, the packets will be stamped with the original dl_src. That is to say, keep the original source mac address.

```
Eg1:
ovs-ofctl add-flow br0 in_port=1,ip,tcp,dl_vlan=2,dl_src=00:11:22:33:44:55,dl_dst=00:01:02:03:04:05,actions=set_fi
send packets
result:

MAC: ------ MAC Header ------
MAC: Destination Address : 00 01 02 03 04 05
MAC: Source Address : 00 11 22 33 44 55

Eg2:
ovs-ofctl add-flow br0 in_port=1,ip,tcp,dl_vlan=2,dl_dst=00:01:02:03:04:05,actions=set_field:0x456-\>tp_src,set_fi
send packets
result:

MAC: ------ MAC Header ------
MAC: Destination Address : 00 01 02 03 04 05
MAC: Source Address : 00 11 22 33 44 55

Eg3:
ovs-ofctl add-flow br0 in_port=1,ip,tcp,dl_vlan=2,dl_src=00:11:22:33:44:55,dl_dst=00:01:02:03:04:05,actions=set_fi
send packets
result:

MAC: ------ MAC Header ------
MAC: Destination Address : 00 01 02 03 04 05
MAC: Source Address : 22 22 22 22 22 22

Eg4:
ovs-ofctl add-flow br0 in_port=1,ip,tcp,dl_vlan=2,dl_dst=00:01:02:03:04:05,actions=set_field:0x456-\>tp_src,set_fi
send packets
result:

MAC: ------ MAC Header ------
MAC: Destination Address : 00 01 02 03 04 05
MAC: Source Address : 22 22 22 22 22 22
```

Configuring option-match-vlan-type

PicOS supports enable/disable option-match-mode-type from version 2.6.5 in Platform P-3922/3924. This function is used to enable or disable matching untagged packets.

Example:

```
admin@PicOS-OVS$ovs-vsctl set-option-match-vlan-type TRUE
  Please reboot for the change to take effect!
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl set-option-match-vlan-type FALSE
  Please reboot for the change to take effect!
admin@PicOS-OVS$
```

If the type is false, PicOS cannot configure one flow entry only matching untagged packets, and cannot configure one flow entry match all tagged packets (tag from1 to 4094). Once option-match-vlan-type is enabled, the flow entry vlan_tci=0x0000/0x1000 can match untagged packets, and flow entry vlan_tci=0x1000/0x1000 can match all tagged packets.

Example:

```
admin@PicOS-OVS$ovs-vsctl set-option-match-vlan-type TRUE
  Please reboot for the change to take effect!
admin@PicOS-OVS$

admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,vlan_tci=0x0000/0x1000,actions=output:12
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=12,vlan_tci=0x1000/0x1000,actions=output:11
```

Send untagged packets to port te-1/1/11, the packets can match the first flow entry and forward on port te-1/1/12. Send tagged packets to port te-1/1/11, the packets cannot match the first flow entry;

Send untagged packets to port te-1/1/12, the packets cannot match the second flow entry; Send tagged (1~4094) packets to port te-1/1/12, the packets can match the second flow entry and forward on port te-1/1/12.

Configuring TTP

TTP means Table Type Pattern.
Before version 2.8.0, the ttp file named as "vz_etech_ttp_v0.3.json." And from version 2.8.0,the ttp json file changed the name to "routing_ttp_v1.0.json",from 3.7.4,the ttp file is named to "picos_ttp.json".
The ttp json file is as following:

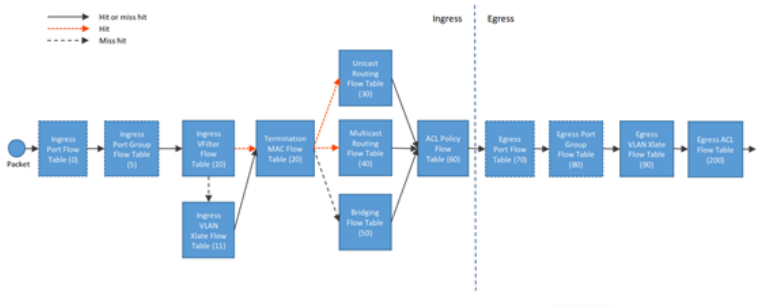


Figure 1:the json file analyse

- Pipeline

```
"table_map": {
    "Ingress_Port_Flow_Table": 0,
    "Ingress_Port_Group_Flow_Table": 5,
    "Ingress_VFilter_Flow_Table": 10,
    "Ingress_VLAN_Xlate_Flow_Table": 11,
    "Termination_MAC_Flow_Table": 20,
    "Unicast_Routing_Flow_Table": 30,
    "Multicast_Routing_Flow_Table": 40,
    "Bridging_Flow_Table": 50,
    "ACL_Policy_Flow_Table": 60,
    "Egress_Port_Flow_Table": 70,
    "Egress_Port_Group_Flow_Table": 80,
    "Egress_VLAN_Xlate_Flow_Table": 90,
    "Egress_ACL_Flow_Table": 200
}
```

Flow Tables

Required flow table:

- Ingress_VFilter_Flow_Table (Required)

  Ingress_VFilter_Flow_Table uses the vcap tcam in hardware, supports QinQ vlan actions.Vcap has the highest priority in VLAN stage.

- Ingress_VLAN_Xlate_Flow_Table (Required)

  Ingress_VLAN_Xlate_Flow_Table uses the VLAN Translation in hardware, supports QinQ vlan actions.

- Termination_MAC_Flow_Table (Required)

  Termination_MAC_Flow_Table add system mac entry in my_station_tcam, to match input packet's service-vlan and dst-mac, and determine whether to route this packet.

- Unicast_Routing_Flow_Table (Required)

  Unicast_Routing_Flow_Table supports match Host and Route IP address.L3 unicast supports ECMP.

- Multicast_Routing_Flow_Table (Required)

  Multicast_Routing_Flow_Table supports l2 ports multicast and l3 multicast.

  L2 ports multicast use “L3 Multicast” group and has no set-field actions.

- Bridging_Flow_Table (Required)

Bridging_Flow_Table supports static mac entries installed by openflow controller and dynamic mac entries if mac-learning enabled.If packet hits a mac entry, the packet will be marked bridging_hit=1.Dynamic mac entry is learned in hardware, and will send an upcall event to software, ovs store the mac entry in bridging table and may notify controller with an experimenter message.

- ACL_Policy_Flow_Table (Required)

  ACL_Policy_Flow_Table uses ICAP TCAM in hardware, can meter, redirect, normal, controller, drop, set-queue, ecmp, etc.

- Egress_VLAN_Xlate_Flow_Table (Required)

  Egress_VLAN_Xlate_Flow_Table uses the egress VLAN Translation in hardware, supports QinQ vlan actions.

- Egress_ACL_Flow_Table (Required)

  Egress_ACL_Flow_Table uses ECAP TCAM in hardware, supports set-dscp, normal, drop actions.Not support matching metadata now.

optional flow table

- Ingress_Port_Flow_Table (Optional)

  Ingress_Port_Flow_Table is the first table in pipeline, represent ingress pipeline start.No flow is allowed to add in this table.

- Ingress_Port_Group_Flow_Table (Optional)

Ingress_Port_Group_Flow_Table matches in_port, and is used to set port ingress port-group id for input port grouping.The port-group is similar to bond port, it is a physical port attribute and can bundle multiple physical ports in a group. Port-group can be used on vlan_xlate table and vfilter flow table, as a match key. Each physical port has a port-group id, default value is 0.

- Egress_Port_Flow_Table (Optional)

  Egress_Port_Flow_Table is the first table in egress pipeline, represent egress pipeline start.No flow is allowed to add in this table.

- Egress_Port_Group_Flow_Table (Optional)

Egress_Port_Group_Flow_Table matches output port (use <in_port> match field), and is used to set port egress port-group id for output port grouping.

Descriptions

Metadata:16-22bits of metadata represents ingress/egress port group.

default-config:You can check the default state using "ovs-vsctl show-port-default-config",admin state is up,config is 0,you can change the state by "ovs-vsctl set-port-default-admin-down true".Need to restart the service after changing the admin state.

default-flood:default state is false,all packets will be dropped if do not matching any flow in flow table.You can change this state by "ovs-vsctl set-port-default-flood true".Need to restart the service after changing the flood state.

Restrictions

- not support ip_ecn in ingress acl match field.
- Do not support following commands “ovs-appctl pica/dump-flows 30””ovs-appctl pica/dump-flows Unicast”
- egress acl table do not support match-mode

TTP Multicast

We will include support for TTP multicast from version 2.8.0. The table number is 40 by default.The pipeline is as follows:

Introduction

The process is different from adding a flow to a unicast routing table. If you add a flow to multicast routing table, you do not need to add the corresponding flows to the VLAN and terminal MAC tables. The switch will check whether the destination MAC of the packet is a multicast address or not. In case its a unicast MAC address, the switch will report an error message. The match fields are Ethernet type, vlan_vid, multicast destination IP address, source IP address. Source ip 0.0.0.0 means (*,g). And (s,g) has the higher priority.

By far, the policy ACL table has ecmp problems in processing the multicast packets coming from multicast routing table.

The multicast routing flow priority is 32768, the IPV4 multicast destination IP address ranges from 224.0.0.0 to 239.255.255.255.The IPV4 destination MAC must begin from 01:00:5e:0…, the IPV6 multicast destination IP address should begin with 0xFF…, the IPV6 multicast destination MAC begins with 33:33…...

Table Description

Multicast Routing table

IPV4 multicast

- **table_id:40**
- **priority:32768**
- **match fields:**

  eth_type:0x0800

  vlan_vid: <vid> 12-bit VLAN id value from header field which Picos support

  IPV4_SRC:<ipv4_src>------IPv4 Unicast Source Address - 32 bits represented as 4 decimal values - nnn.nnn.nnn.nnn

  IPV4_DST:<ipv4_mc>------valid value is from 224.0.0.0 to 239.255.255.255
- **instructions**

  goto_table:60 (optional)

  write_actions(necessary): L3 Multicast group,DEC_NW_TTL

IPV6 multicast

- **table_id:40**
- **priority:32768**
- **match fields:**

  eth_type:0x86dd

  vlan_vid: <vid> 12-bit VLAN id value from header field which Picos support

  IPV6_SRC:<ipv6_src>------IPv6 Unicast Source Address - 128 bits represented as 8 groups of hex quartets - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

  IPV6_DST:<ipv6_mc>------valid value is ff00:0:0:0:0:0:0:0,mask is ff00:0:0:0:0:0:0:0
- **instructions**

  goto_table:60 (optional)
  write_actions(necessary): L3 Multicast group,DEC_NW_TTL

default flows in multicast routing table

- **priority:32768**
- **match fields:[ ]**
- **instructions:**

  goto_table:policy table(table_id is 60)

ACL table

match fields:all the match fields the same with tcam in non-TTP mode.

instructions:write_actions,

actions: L2 interface group |L2 Rewrite group | L3 ECMP group | output:controller ,all these actions can not exist at the same time ,only one kind of group exist.

POP_VLAN(optional)

SET_QUEUE(optional)

modify DSCP(optional)

Default flow in ACL table is pass.

> **l2 multicast and l3 multicast**
> l2 multicast:the field "dec_nw_ttl" can not work,but in flow,dec_nw_ttl is the neccessary.
>
> l3 multicast:del_nw_dec field is neccessary and works as well

> **Multicast table and Acl table can not be matched at the same time.If packets match multicast table,can not match the acl table at the same time unless not match the multicast table.**

Groups Description

L2 Interface group

group type is ***indirect***,and action only support output port.

L3 Multicast Interface group

group type is ***indirect,***actions is modify src mac and vlan,**output** is a "L2 Interface group group".

L3 Multicast group

group type is ***all***,bucket is a ***"L3 Multicast Interface group" or "L2 Interface group"***

Examples

Example 1: IPv4 Multicast (l3 multicast)

(1)configure ttp

```
ovs-vsctl set-ttp-enable true
ovs-vsctl set-ttp-file picos_ttp.json
ovs-vsctl show-ttp
sudo systemctl restart picos
```

(2)configure bridge and port

```
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set interface ge-1/1/3 type=pica8
```

(3)add groups

l2 interface group:

```
ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:2
ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=output:3
```

l3 multicast interface:

```
ovs-ofctl add-group br0 group_id=3,type=indirect,bucket=set_field:88:88:88:00:00:00-\>dl_src,set_field:200-\>vlan_
ovs-ofctl add-group br0 group_id=4,type=indirect,bucket=set_field:44:44:44:00:00:00-\>dl_src,set_field:300-\>vlan_
```

l3 multicast group:

```
ovs-ofctl add-group br0 group_id=5,type=all,bucket=group:3,bucket=group:4
```

(4)add flow

Here,flows' action ***goto_table:60*** is optional.

```
ovs-ofctl add-flow br0 table=40,priority=32768,dl_type=0x0800,dl_vlan=10,nw_src=192.168.1.100,nw_dst=234.234.245.2
```

(5)check the hardware flow table

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
Multicast Routing Table: (Total 1 flows)
 ID=12 ip,dl_vlan=10,nw_src=192.168.1.100,nw_dst=234.234.245.245, actions:group(id=3,all,n=2,b0(group(id=2,indirec
```

(6) send multicast packets

send packets with dst mac "01:00:5E:07:88:88",vlan is 10,dst multicast ipv4 address is 234.234.245.245.

Then ge-1/1/2 will transmit the packets with vlan 200,src mac is 88:88:88:00:00:00,ge-1/1/3 will transmit the packets is src mac is 44:44:44:00:00:00,vlan is 300

Example 2: IPv4 Multicast (l2 multicast)

(1)enable TTP and add bridge and port first.

(2)**Add group**

l2 interface group:

```
ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:2
```

l3 multicast group:

```
ovs-ofctl add-group br0 group_id=3,type=all,bucket=group:1
```

(3)add flow

```
ovs-ofctl add-flow br0 table=40,priority=32768,dl_type=0x0800,dl_vlan=10,nw_src=192.168.1.100,nw_dst=234.234.245.24
```

(4)**Check the hardware flow**

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
Multicast Routing Table: (Total 1 flows)
 ID=10 ip,dl_vlan=10,nw_src=192.168.1.100,nw_dst=234.234.245.245, actions:group(id=3,all,n=1,b0(live,group(id=1,inc
```

(5)send packets

send packets with dst mac "01:00:5E:07:88:88",vlan is 10,dst multicast ipv4 address is 234.234.245.245.

Then ge-1/1/2 will transmit the packets which are the sane with the packets from ge-1/1/1.

Example 3: IPv6 Multicast(l3 multicast)

(1) enable TTP and add port and bridge.

(2)add group

l2 interface group:

```
ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:2
ovs-ofctl add-group br0 group_id=5,type=indirect,bucket=output:3
```

l3 multicast interface group:

```
ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=set_field:88:88:88:00:00:00-\>dl_src,set_field:200-\>vlan_\
ovs-ofctl add-group br0 group_id=6,type=indirect,bucket=set_field:44:44:44:00:00:00-\>dl_src,set_field:300-\>vlan_\
```

l3 multicast group:

```
ovs-ofctl add-group br0 group_id=3,type=all,bucket=group:2,bucket=group:6
```

(3) add flow

```
ovs-ofctl add-flow br0 table=40,priority=32768,dl_type=0x86dd,dl_vlan=10,ipv6_src=2000::1,ipv6_dst=ff00::1,actions=
```

(4)**Check the hardware flow**

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
Multicast Routing Table: (Total 1 flows)
 ID=5040 ipv6,dl_vlan=10,ipv6_src=2000::1,ipv6_dst=ff00::1, actions:group(id=3,all,n=2,b0(live,group(id=2,indirect
```

(5)send ipv6 mutlicast packets

send ipv6 packets with dst mac 33:33:33:00:00:01,vlan is 10,ipv6 src address is 2000::1,ipv6 dst address is ff00::1

Then ge-1/1/2 will transmit the packets with source mac 88:88:88:00:00:00,vlan is 200,ge-1/1/3 will transmit the packets with dst mac is 33:33:33:00:00:01,src mac is 44:44:44:00:00:00, vlan is 300.

Example 4: IPv6 Multicast (l2 multicast)

(1) enable TTP and add bridge and port

(2)add groups

l2 interface group:

```
ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:2
ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=output:3
```

l3 multicast group:

```
ovs-ofctl add-group br0 group_id=3,type=all,bucket=group:1,bucket=group:2
```

(3)add flow

```
ovs-ofctl add-flow br0 table=40,priority=32768,dl_type=0x86dd,dl_vlan=10,ipv6_src=2000::1,ipv6_dst=ff00::1,actions=
```

(4)check the hardware flow

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
Multicast Routing Table: (Total 1 flows)
 ID=1 ipv6,dl_vlan=10,ipv6_src=2000::1,ipv6_dst=ff00::1, actions:group(id=3,all,n=2,b0(group(id=1,indirect,n=1,b0(
```

(5)send ipv6 packets

send ipv6 packets with dst mac 33:33:33:00:00:01,src mac is 22:11:11:11:11:11,vlan is 10,ipv6 src address is 2000::1,ipv6 dst address is ff00::1

Then ge-1/1/2 and ge-1/1/3 will transmit the packets with source mac 22:11:11:11:11:11,vlan is 10.

TTP Unicast

Introduction

This document describes the Table Type Pattern (TTP) and its usage.

TTP defines a template of tables that can be configured using open flow. It uses JSON notation to define the data structure for the pipeline defined in the TTP. Open flow instructions can use the parameters defined in the TTP file to program the flows. If a flow cannot be configured, the switch will report an error message.

Enabling TTP Mode

From PicOS version 2.7.1, supporting for TTP mode has been added in our switches. To use the TTP mode, user must first enable this mode. To enable the TTP mode, use the command ***"ovs-vsctl set-ttp-enable true"*** . To add the TTP file, use the command ***"ovs-vsctl set-ttp-file <TTP file>.json".*** After adding the file, restart the switch and the TTP mode should be enabled on the switch.From version 3.7.4,add some flow tables(bridging flow table,Egress_Port_Flow_Table,Egress_Port_Group_Flow_Table,Egress_VLAN_Xlate_Flow_Table,Egress_ACL_Flow_Table)

json file
About .JSON FILE:

- Only "table_map" and "flow_tables" can be modified.
- "table_map": User can modify the table number of "VLAN," "Termination MAC," "Unicast Routing" and "Policy ACL". All of the four table id's must be increasing and different. For example, if user wants table 20 to be the VLAN table, write like this "VLAN:" 20 and so on.
- Flow_tables: Only the priority of all the flows tables can be changed. If user modifies vlan filter tables' priority to 1999, when user adds a flow, user must specify that the priority is 1999.
- path: /ovs/share/openvswitch

At present, users cannot modify the json file. If necessary, users may notify our team, and we may be able to change it.

Table map is:

- "Ingress_Port_Flow_Table": 0,
- "Ingress_Port_Group_Flow_Table": 5,
- "Ingress_VFilter_Flow_Table": 10,
- "Ingress_VLAN_Xlate_Flow_Table": 11,
- "Termination_MAC_Flow_Table": 20,
- "Unicast_Routing_Flow_Table": 30,
- "Multicast_Routing_Flow_Table": 40,
- "Bridging_Flow_Table": 50,
- "ACL_Policy_Flow_Table": 60,
- "Egress_Port_Flow_Table": 70,
- "Egress_Port_Group_Flow_Table": 80,
- "Egress_VLAN_Xlate_Flow_Table": 90,
- "Egress_ACL_Flow_Table": 200

Notification

- In the acl table, if any layer 2 header content of packets is modified, previous actions in route table will be invalid.
- At present, the packets can ecmp in src ip by default.

Table match and instructions

Ingress_Port_Group_Flow_Table:

Match:in_port

Actions: write_metadata(bit16-22: Port Group [0-127]),goto_table: Ingress_VFilter_Flow_Table

Built-in:

Match:[]

Actions: write_metadata:0,goto_table: Ingress_VFilter_Flow_Table

```
ovs-ofctl add-flow br0 table=5,priority=32768,in_port=1,actions=write_metadata:0x20000/0x7f0000,goto_table:10
```

Ingress_VFilter_Flow_Table:

Match:none or metadata or in_port,Of course you can match “priority,in_port,vlan_vid,dl_vlan_pcp,dl_type” at the same time.

Note:metadata and in_port should better not match at the same time.

Actions:push_vlan,goto_table:Termination_MAC_Flow_Table

built-in:

Match:[]

Actions:goto_table:Termination_MAC_Flow_Table

```
ovs-ofctl add-flow br0 table=10,actions=push_vlan:0x8100,set_field:200-\>vlan_vid,push_vlan:0x8100,set_field:300-\>
ovs-ofctl add-flow br0 table=10,priority=32768,metadata=0x000002/0x7f0000,vlan_vid=0x064/0x0ff,dl_vlan_pcp=4,dl_typ
ovs-ofctl add-flow br0 table=10,priority=32768,in_port=1,vlan_vid=0x064/0x0ff,dl_vlan_pcp=4,dl_type=0x0800,actions=
```

Ingress_VLAN_Xlate_Flow_Table

QinQ ingress vlan xlate table for packets, table size is 4K

Match: metadata,vlan_vid

Actions: push_vlan(optional), set_field vlan,goto “Termination_MAC_Flow_Table”

Built-in: goto “Termination_MAC_Flow_Table”

```
ovs-ofctl add-flow br0 table=11,priority=32768,metadata=0x000002/0x7f0000,dl_vlan=100,actions=push_vlan:0x8100,set_
```

Termination_MAC_Flow_Table

In this table, the user can configure a flow to decide if the packets go to the route table or not,do not support a output port in this table. By default, packets will go to the bridging flow table directly, instead of going to route table first. The match fields of the flow supported by this table are dl_dst, dl_vlan, action is goto_table:30. Multicast and broadcast MAC are not supported here.

Match:eth_dst,vlan_vid

Actions:goto “Unicast_Routing_Flow_Table”

Built-in: goto “Bridging_Flow_Table”

```
ovs-ofctl add-flow br-s table=20,priority=32768,dl_dst=00:11:22:33:44:56,dl_vlan=2015,actions=goto_table:30
```

Unicast_Routing_Flow_Table

In this table, users can direct the packets' route through several different kind of groups by means of writing actions. The matching fields are dl_type, nw_dst, actions are several kinds of groups and dec_nw_ttl, then go to ACL table. According our .json file we can add this kind of flow. Broadcast and multicast are not supported in this table. By default,all packets pass through this table and goto acl table.

Match:dl_type,nw_dst/ipv6_dst(optional)

Actions:clear_actions or controller or L3 Unicast/L3 ecmp group,goto_table:60(necessary)

Built-in:goto_table: ACL_Policy_Flow_Table

```
ovs-ofctl add-flow br0 table=30,priority=32768,dl_type=0x0800,nw_dst=192.168.1.100,actions=output:controller,goto_
```

example1:

```
step1,add group
#########add l2 interface group:
ovs-ofctl add-group br0 group_id=1,type=indirect,bucket=output:2

#########add l3 unicast group:
ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=set_field:66:66:66:11:11:11-\>dl_src,set_field:88:88:88:11

Step2,delete route flow and add another flow
ovs-ofctl add-flow br0 table=20,priority=32768,dl_vlan=100,dl_dst=22:22:22:22:22:22,actions=goto_table:30
ovs-ofctl add-flow br0 table=30,priority=32768,dl_type=0x0800,nw_dst=192.168.1.100,actions=write_actions\(group:2,

step3,check the flows
ovs-ofctl dump-flows br0
ovs-appctl pica/dump-flows

step4,send packets
send 10000 packets with vlan 100,dst mac is 22:22:22:22:22:22,dst ip is 192.168.1.100 to te-1/1/1.

Result:te-1/1/2 should transmit packets with vlan 3000,dst mac is 88:88:88:11:11:11,src mac is 66:66:66:11:11:11,t
```

Example2

User can also complete the ecmp through a select group.

L2 interface group:

```
ovs-ofctl add-group br-s group_id=1,type=indirect,bucket=output:77
 ovs-ofctl add-group br-s group_id=5,type=indirect,bucket=output:79
```

L3 UNICAST group:

```
ovs-ofctl add-group br-s group_id=2,type=indirect,bucket=set_field:66:66:66:00:00:00-\>dl_src,set_field:66:66:66:1
ovs-ofctl add-group br-s group_id=6,type=indirect,bucket=set_field:22:11:11:11:11:11-\>dl_src,set_field:44:44:44:1
```

L3 ff group:

```
ovs-ofctl add-group br-s group_id=3,type=fast_failover,bucket=group:2,watch_port:77
ovs-ofctl add-group br-s group_id=7,type=fast_failover,bucket=group:6,watch_port:79
```

L3 ecmp:

```
ovs-ofctl add-group br-s group_id=4,type=select,bucket=group:2,bucket=group:7
```

Add flow and check:

```
ovs-ofctl add-flow br-s table=30,priority=32768,dl_type=0x0800,nw_dst=192.168.1.100,actions=write_actions\(group:4
admin@PicOS-OVS$ovs-ofctl dump-flows br-s
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=76.544s, table=30, n_packets=n/a, n_bytes=n/a, ip,nw_dst=192.168.1.100 actions=write_actions
admin@PicOS-OVS$ovs-appctl pica/dump-flows
Ingress Port Table: (Total 0 flows)

VLAN Table: (Total 0 flows)

Termination MAC Table: (Total 0 flows)

Unicast Routing Table: (Total 1 flows)
 ID=1 ip,nw_dst=192.168.1.100, actions:group(id=9,select,n=2,b0(live,group(id=3,ff,n=1,b0(live,group(id=2,indirect

Policy ACL Table: (Total 0 flows)
```

Bridging_Flow_Table

When Mac-Learning is enabled on the chip, the entries for unicast forwarding are automatically learned, updated(station-move) and deleted(idle-timeout)." To be installed/updated/deleted via FlowMod(ADD/MODIFY/MODIFY_STRICT/DELETE).

Match:eth_dst,vlan_vid

Actions:output_port,goto_table: ACL_Policy_Flow_Table

Built-in: goto_table: ACL_Policy_Flow_Table

```
ovs-ofctl add-flow br0 table=50,priority=32768,dl_dst=44:44:44:44:44:44,dl_vlan=2000,actions=write_actions\(output
```

send packets matching above flow with dst mac 44:44:44:44:44:44,vlan 2000 to te-1/1/1.

Result: te-1/1/2 should transmit the packets.

ACL_Policy_Flow_Table

In this table, users can add a flow with any match field supported by our switch. The actions could be meter, group, controller, drop, set_queue.

Match:in_port,mpls,vlan,mac,ip,inner_vlan_vid,inner_vlan_pcp,sctp,mpls_label2etc.All the match fields are optional.

Actions:meter(optional),pop_l2mpls(optional),pop_mpls(optional),push_l2mpls,set_field:mpls_label(optional),group,output_port,and so on.

Built-in: goto_table:Egress_VLAN_Xlate_Flow_Table

```
ovs-ofctl add-flow br0 table=60,in_port=1,dl_vlan=2000,dl_dst=44:33:22:11:00:00,mpls,mpls_label=16,mpls_tc=3,mpls_l
```

```
ovs-ofctl add-flow br-s table=60,priority=65535,in_port=78,dl_type=0x86dd,dl_src=22:22:22:22:22:22,dl_dst=44:44:44
```

```
ovs-ofctl add-flow br-s table=60,actions=write_actions\(group:4\)
```

Egress_VLAN_Xlate_Flow_Table

This entry is for converting outgoing Tagged packets from QinQ to Single Tagged or untagged.

Match:metadata,vlan_vid,inner_vlan_vid

actions:pop_vlan,set_field:vlan,goto_table:Egress_ACL_Flow_Table

built-in: goto_table:Egress_ACL_Flow_Table

```
ovs-ofctl add-flow br0 table=90,priority=32768,metadata=0x20000/0x7f0000,dl_vlan=2000,inner_vlan_vid=1000,actions=
```

Egress_ACL_Flow_Table

match: IN_PORT,OUTPUT_PORT, ETH_DST/ ETH_SRC, ETH_TYPE, VLAN_VID/ VLAN_PCP,TCP/UDP,SCTP，etc.

actions:set_field:ip_dscp, clear_actions, output:normal

####add flow in ingress acl ####

```
ovs-ofctl add-flow br0 table=60,in_port=1,actions=write_actions\(output:2\)
```

####add flow in egress acl

```
ovs-ofctl add-flow br0 table=200,in_port=1,dl_dst=22:22:22:22:22:22,dl_src=22:11:11:11:11:11,dl_vlan=2000,dl_vlan_
```

send packets

a,send packets with dst mac 22:22:22:22:22:22,src mac 22:11:11:11:11:11,pcp is 3 to te-1/1/1.

b,send packets with dst mac 22:22:22:22:22:22,src mac 22:11:11:11:11:11,pcp is 0 to te-1/1/1.

Result:

a,te-1/1/2 should drop packets.

b,te-1/1/2 should transmit the packets.

List TTP System Resources Usage

From version 2.8.0, when ttp is enabled,we can use command ovs-appctl pica/show tables to check max limitation or current used of different tables.

```
admin@PICOS-OVS:~$ ovs-appctl pica/show tables
TTP Tables Statistics:
    TTP Tables                    Max Limitation          Current Used
    ------------------------------------------------------------------------
    Ingress Port Group Table        1024                    0
    Ingress VFilter Table           510                     0
    Ingress VLAN Xlate Table        4096                    0
    Termination MAC Table           510                     0
    Unicast Routing Table (Host)    12000                   IPv4(0),IPv6(0*2)
    Unicast Routing Table (Route)   12000                   IPv4(0),IPv6(0*2)
    Multicast Routing Table         6400                    IPv4(0),IPv6(0)
    Bridging Table                  32256                   0
    Policy ACL Table                2046                    0
    Egress Port Group Table         1024                    0
    Egress VLAN Xlate Table         4096                    0
    Egress ACL Table                510                     0
admin@PICOS-OVS:~$
```

Picos_ttp.json

Click here to expand...


```
{
"NDM_metadata": {
"authority": "Pica8, Inc",
"OF_protocol_version": "1.3.4",
"type": "TTPv1",
"name": "PICOS_TTP",
"version": "2.0.0",
"doc": [
"A TTP supporting QinQ, mac-learning, l3, ecmp, acl and egress."
]
},
"features": [],
"table_map": {
"Ingress_Port_Flow_Table": 0,
"Ingress_Port_Group_Flow_Table": 5,
"Ingress_VFilter_Flow_Table": 10,
"Ingress_VLAN_Xlate_Flow_Table": 11,
"Termination_MAC_Flow_Table": 20,
"Unicast_Routing_Flow_Table": 30,
"Multicast_Routing_Flow_Table": 40,
"Bridging_Flow_Table": 50,
"ACL_Policy_Flow_Table": 60,
"Egress_Port_Flow_Table": 70,
"Egress_Port_Group_Flow_Table": 80,
"Egress_VLAN_Xlate_Flow_Table": 90,
"Egress_ACL_Flow_Table": 200
},
"identifiers": {
"Identifier list": [
{
"var": "<port_no>",
"doc": [
"ifNum, 32-bit value. A valid port number Picos support."
]
},
{
"var": "<reserved_port>",
"doc": [
"ifNum, 32-bit value. Openflow reserved ports: CONTROLLER, NORMAL, LOCAL, IN_PORT, FLOOD, ALL."
]
},
{
"var": "<metadata>",
"doc": [
"Metadata list:",
" - bit0: Reserved.",
" - bit1: Bridging_HIT (Marked when a packet hits Bridging Entry.)",
" - bit2: Unicast_Routing_HIT (Marked when a packet hits UC Routing Entry.)",
" - bit3: Multicast_Routing_HIT (Marked when a packet hits UC Host or MC Routing Entry.)",
" - bit16-22: Port Group[0-127] (A group that bundles multiple OpenFlow ports. It is used on VLAN Flow Tables as a match key. 7bits, modified in
Ingress/Egress_Port_Group_Flow_Table. e.g. metadata=0x20000/0x7f0000 means port-group 2)",
" - others: Reserved."
]
},
{
"var": "<eth_dst>",
"doc": "Any valid ethernet destination address."
},
{
"var": "<eth_src>",
"doc": "Any valid ethernet source address."
},
{
"var": "<mac_uc>",
"doc": "Any valid unicast mac address."
},
{
"var": "<eth_type>",
"doc": [
"Any valid ethertype, which will be >1536 (0x0600),",
"except for 0x8870 (jumbo frame)"
]
},
{
"var": "<mpls_label>",
"doc": "All valid mpls label Picos support."
},
{
```

```
"var": "<mpls_tc>",
"range": "0..7",
"doc": "Mpls exp field, used as CoS."
},
{
"var": "<mpls_ttl>",
"doc": "Mpls ttl value."
},
{
"var": "<vlan_vid>",
"doc": [
"12-bit VLAN id value from header field which Picos support.",
"OpenFlow sets bit 12 to indicate presence of the field."
]
},
{
"var": "<vlan_pcp>",
"range": "0..7",
"doc": "VLAN header PCP field"
},
{
"var": "<inner_vlan_vid>",
"doc": [
"PICOS experimenter.",
"12-bit Inner-vlan id value from header field which Picos support.",
"OpenFlow sets bit 12 to indicate presence of the field."
]
},
{
"var": "<inner_vlan_pcp>",
"range": "0..7",
"doc": "Inner-vlan header PCP field, PICOS experimenter."
},
{
"var": "<ip_dscp>",
"range": "0..255",
"doc": "IP Header DSCP field."
},
{
"var": "<ip_proto>",
"doc": "All valid ip protocol Picos support."
},
{
"var": "<ipv4_src>",
"doc": "IPv4 Source Address - 32 bits represented as 4 decimal values - nnn.nnn.nnn.nnn"
},
{
"var": "<ipv4_dst>",
"doc": "IPv4 Destination Address - 32 bits represented as 4 decimal values - nnn.nnn.nnn.nnn"
},
{
"var": "<ipv4_uc>",
"doc": "IPv4 Unicast Address - 32 bits represented as 4 decimal values - nnn.nnn.nnn.nnn"
},
{
"var": "<ipv4_mc>",
"doc": "IPv4 Multicast Address - 32 bits represented as 4 decimal values - nnn.nnn.nnn.nnn"
},
{
"var": "<ipv6_src>",
"doc": "IPv6 Source Address - 128 bits represented as 8 groups of hex quartets - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn"
},
{
"var": "<ipv6_dst>",
"doc": "IPv6 Destination Address - 128 bits represented as 8 groups of hex quartets - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn"
},
{
"var": "<ipv6_uc>",
"doc": "IPv6 Unicast Address - 128 bits represented as 8 groups of hex quartets - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn"
},
{
"var": "<ipv6_mc>",
"doc": "IPv6 Multicast Address - 128 bits represented as 8 groups of hex quartets - nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn"
},
{
"var": "<tp_src>",
"range": "1..65535",
"doc": "16-bit Transmition source port, tcp/udp/sctp"
},
{
"var": "<tp_dst>",
"range": "1..65535",
"doc": "16-bit Transmition destination port, tcp/udp/sctp"
},
{
"var": "<icmpv4_type>",
"doc": "All valid icmpv4_type"
},
```

```
{
"var": "<icmpv4_code>",
"doc": "All valid icmpv4_code"
},
{
"var": "<icmpv6_type>",
"doc": "All valid icmpv6_type"
},
{
"var": "<icmpv6_code>",
"doc": "All valid icmpv6_code"
},
{
"var": "<queue_id>",
"doc": "All valid queue_id"
},
{
"var": "<group_id>",
"doc": "All valid group_id"
},
{
"var": "<meter_id>",
"range": "1..65535",
"doc": "Meter id for a Policy ACL meter."
},
{
"var": "<rate>",
"doc": [
"By default this value is all rate Picos support.",
"User could redefine it such as 1..100000 kbps."
]
},
{
"var": "<burst>",
"doc": [
"By default this value is all burst Picos support.",
"User could redefine it such as 1..100000 kbits."
]
}
]
},
"meter_table": {
"meter_types": [
{
"name": "Drop Meter Type",
"bands": [
{
"type": "DROP",
"rate": "<rate>",
"burst": "<burst>"
}
]
},
{
"name": "DSCP Remark Meter Type",
"bands": [
{
"type": "DSCP_REMARK",
"rate": "<rate>",
"burst": "<burst>"
}
]
}
],
"built_in_meters": []
},
"flow_tables": [
{
"name": "Ingress_Port_Flow_Table",
"doc": [
"First table in pipeline, represent ingress pipeline start.",
"No flow is allowed to add in this table."
],
"flow_mod_types": [],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Ingress_Port_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Ingress_Port_Group_Flow_Table"
}
```

```
]
}
]
},
{
"name": "Ingress_Port_Group_Flow_Table",
"doc": [
"Match in port, table size is ports num + 1.",
"Input port ingress Grouping."
],
"flow_mod_types": [
{
"name": "Ingress Port Group",
"priority": "32768",
"doc": [
"Bundles multiple OpenFlow ports in a group."
],
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "WRITE_METADATA",
"metadata": "<metadata>",
"doc": [
"bit16-22: Port Group [0-127]"
]
},
{
"instruction": "GOTO_TABLE",
"table": "Ingress_VFilter_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Ingress_Port_Group_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "WRITE_METADATA",
"metadata": "<metadata>",
"doc": [
"metadata: port_group = 0"
]
},
{
"instruction": "GOTO_TABLE",
"table": "Ingress_VFilter_Flow_Table"
}
]
}
]
},
{
"name": "Ingress_VFilter_Flow_Table",
"doc": [
"QinQ vlan vfilter table for packets, table size is 1K.",
"Valid metadata should use port-group in this table, and is conflict with in_port."
],
"flow_mod_types": [
{
"name": "VFilter VLAN Conversion",
"priority": "0..65535",
"doc": [
"This flow entry is for converting incoming packet to QinQ packet."
],
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "METADATA",
"value": "<metadata>",
"match_type": "mask"
},
```

```
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "mask"
},
{
"field": "VLAN_PCP",
"value": "<vlan_pcp>",
"match_type": "all_or_exact"
},
{
"field": "ETH_TYPE",
"value": "<eth_type>",
"match_type": "all_or_exact"
}
],
"instruction_set": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "PUSH_VLAN"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_PCP",
"value": "<vlan_pcp>"
}
]
},
{
"zero_or_one": [
{
"action": "PUSH_VLAN"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_PCP",
"value": "<vlan_pcp>"
}
]
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "Termination_MAC_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Ingress_VFilter_Flow_Table."
],
"match_set": [],
```

```
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Ingress_VLAN_Xlate_Flow_Table"
}
]
}
]
},
{
"name": "Ingress_VLAN_Xlate_Flow_Table",
"doc": [
"QinQ ingress vlan xlate table for packets, table size is 4K."
],
"flow_mod_types": [
{
"name": "Tagged VLAN Conversion",
"priority": "32768",
"doc": [
"This flow entry is for converting incoming tagged packets to QinQ packets."
],
"match_set": [
{
"field": "METADATA",
"value": "<metadata>",
"match_type": "mask"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "PUSH_VLAN"
}
]
},
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "Termination_MAC_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Ingress_VLAN_Xlate_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Termination_MAC_Flow_Table"
}
]
}
]
},
{
"name": "Termination_MAC_Flow_Table",
"doc": [
"Determine whether to route a packet, table size is 512."
],
"flow_mod_types": [
{
"name": "L3 Unicast MAC",
"priority": "32768",
"doc": [
"System mac for L3 unicast routing."
],
```

```
"match_set": [
{
"field": "ETH_DST",
"value": "<mac_uc>",
"match_type": "exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Unicast_Routing_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Termination_MAC_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Bridging_Flow_Table"
}
]
}
]
},
{
"name": "Unicast_Routing_Flow_Table",
"doc": [
"Supports match Host and Route IP address."
],
"flow_mod_types": [
{
"name": "IPv4 Unicast Host",
"priority": "32768",
"doc": [
"Matches IPv4 unicast host address."
],
"match_set": [
{
"field": "ETH_TYPE",
"value": "0x0800",
"match_type": "exact"
},
{
"field": "IPV4_DST",
"value": "<ipv4_uc>",
"match_type": "exact"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "CONTROLLER"
}
]
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
```

```
{
"exactly_one": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
},
{
"action": "DEC_NW_TTL"
}
]
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
},
{
"name": "IPv4 Unicast LPM",
"priority": "32768",
"doc": [
"Matches IPv4 unicast route address."
],
"match_set": [
{
"field": "ETH_TYPE",
"value": "0x0800",
"match_type": "exact"
},
{
"field": "IPV4_DST",
"value": "<ipv4_uc>",
"match_type": "prefix"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "CONTROLLER"
}
]
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"exactly_one": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
},
{
"action": "DEC_NW_TTL"
}
]
}
]
},
```

```
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
},
{
"name": "IPv6 Unicast Host",
"priority": "32768",
"doc": [
"Matches IPv6 unicast host address."
],
"match_set": [
{
"field": "ETH_TYPE",
"value": "0x86dd",
"match_type": "exact"
},
{
"field": "IPV6_DST",
"value": "<ipv6_uc>",
"match_type": "exact"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "CONTROLLER"
}
]
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"exactly_one": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
},
{
"action": "DEC_NW_TTL"
}
]
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
},
{
"name": "IPv6 Unicast LPM",
"priority": "32768",
"doc": [
"Matches IPv6 unicast route address."
],
"match_set": [
{
"field": "ETH_TYPE",
"value": "0x86dd",
"match_type": "exact"
},
{
```

```
"field": "IPV6_DST",
"value": "<ipv6_uc>",
"match_type": "prefix"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "CONTROLLER"
}
]
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"exactly_one": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
},
{
"action": "DEC_NW_TTL"
}
]
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default",
"priority": "32768",
"doc": [
"Default pass through, Policy ACL forward or packet dropped."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
}
]
},
{
"name": "Multicast_Routing_Flow_Table",
"doc": [
"Supports exact match on IP destination address",
"VLAN id values must be consistent"
],
"flow_mod_types": [
{
"name": "IPv4 Multicast",
"priority": "32768",
"doc": [
"IPv4 Multicast"
],
"match_set": [
```

```
{
"field": "ETH_TYPE",
"value": "0x0800",
"match_type": "exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
},
{
"field": "IPV4_SRC",
"value": "<ipv4_uc>",
"match_type": "all_or_exact"
},
{
"field": "IPV4_DST",
"value": "<ipv4_mc>",
"match_type": "exact",
"const_mask": "224.0.0.0",
"const_value": "224.0.0.0"
}
],
"instruction_set": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"action": "GROUP",
"group_id": "L3 Multicast"
},
{
"action": "DEC_NW_TTL"
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
},
{
"name": "IPv6 Multicast",
"priority": "32768",
"doc": [
"IPv6 Multicast"
],
"match_set": [
{
"field": "ETH_TYPE",
"value": "0x86dd",
"match_type": "exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
},
{
"field": "IPV6_SRC",
"value": "<ipv6_uc>",
"match_type": "all_or_exact"
},
{
"field": "IPV6_DST",
"value": "<ipv6_mc>",
"match_type": "exact",
"const_mask": "ff00:0:0:0:0:0:0:0",
"const_value": "ff00:0:0:0:0:0:0:0"
}
],
"instruction_set": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"action": "GROUP",
"group_id": "L3 Multicast"
},
{
"action": "DEC_NW_TTL"
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
```

```
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default",
"priority": "32768",
"doc": [
"Default pass through, Policy ACL forward or packet dropped."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
}
]
},
{
"name": "Bridging_Flow_Table",
"doc": [
"When Mac-Learning is enabled on the chip, the entries for unicast forwarding are automatically learned, updated(station-move) and deleted(idle-timeout).",
"To be installed/updated/deleted via FlowMod(ADD/MODIFY/MODIFY_STRICT/DELETE)."
],
"flow_mod_types": [
{
"name": "Known-MAC",
"priority": "32768",
"doc": "Type used to create an entry for a learned MAC.",
"match_set": [
{
"field": "ETH_DST",
"value": "<mac_uc>",
"match_type": "exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "<port_no>"
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "MAC Learning",
"priority": "32768",
"doc": [
"When Mac-Learning is enabled on the chip, the entries for unicast forwarding are automatically learned, updated(station-move) and deleted(idle-timeout)."
],
"match_set": [
{
"field": "ETH_DST",
"value": "<mac_uc>",
"match_type": "exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"action": "OUTPUT",
"port": "<port_no>"
}
```

```
]
},
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
},
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Bridging_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "ACL_Policy_Flow_Table"
}
]
}
]
},
{
"name": "ACL_Policy_Flow_Table",
"doc": [
"Match on variety of fields.",
"Can meter, redirect, drop, set-queue, etc.",
"METADATA match field should not be used if flow action is TO_CPU."
],
"flow_mod_types": [
{
"name": "IPv4 Mode",
"priority": "0..65535",
"doc": [
"IPv4 mode."
],
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "METADATA",
"value": "<metadata>",
"match_type": "mask"
},
{
"field": "ETH_DST",
"value": "<eth_dst>",
"match_type": "mask"
},
{
"field": "ETH_SRC",
"value": "<eth_src>",
"match_type": "mask"
},
{
"field": "ETH_TYPE",
"value": "<eth_type>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_PCP",
"value": "<vlan_pcp>",
"match_type": "all_or_exact"
},
{
"field": "MPLS_LABEL",
"value": "<mpls_label>",
"match_type": "all_or_exact"
},
{
"field": "MPLS_TC",
"value": "<mpls_tc>",
"match_type": "all_or_exact"
},
{
"field": "MPLS_LABEL2",
"value": "<mpls_label>",
```

```
"match_type": "all_or_exact"
},
{
"field": "IP_DSCP",
"value": "<ip_dscp>",
"match_type": "all_or_exact"
},
{
"field": "IP_PROTO",
"value": "<ip_proto>",
"match_type": "all_or_exact"
},
{
"field": "IPV4_SRC",
"value": "<ipv4_src>",
"match_type": "mask"
},
{
"field": "IPV4_DST",
"value": "<ipv4_dst>",
"match_type": "mask"
},
{
"field": "TCP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "TCP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "UDP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "UDP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "SCTP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "SCTP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "ICMPV4_TYPE",
"value": "<icmpv4_type>",
"match_type": "all_or_exact"
},
{
"field": "ICMPV4_CODE",
"value": "<icmpv4_code>",
"match_type": "all_or_exact"
},
{
"field": "INNER_VLAN_VID",
"value": "<inner_vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "INNER_VLAN_PCP",
"value": "<inner_vlan_pcp>",
"match_type": "all_or_exact"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "METER",
"meter_id": "<meter_id>"
}
]
},
{
"zero_or_one": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
```

```
"zero_or_one": [
{
"action": "POP_L2MPLS"
},
{
"action": "POP_MPLS"
}
]
},
{
"zero_or_one": [
{
"action": "PUSH_L2MPLS"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "MPLS_LABEL",
"value": "<mpls_label>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "MPLS_TC",
"value": "<mpls_tc>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_MPLS_TTL",
"value": "<mpls_ttl>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_SRC",
"value": "<eth_src>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_DST",
"value": "<eth_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"zero_or_one": [
{
"action": "PUSH_MPLS"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "MPLS_LABEL",
"value": "<mpls_label>"
}
]
},
{
"zero_or_one": [
{
```

```
"action": "SET_FIELD",
"field": "MPLS_TC",
"value": "<mpls_tc>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_MPLS_TTL",
"value": "<mpls_ttl>"
}
]
},
{
"zero_or_one": [
{
"action": "PUSH_MPLS"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "MPLS_LABEL",
"value": "<mpls_label>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "MPLS_TC",
"value": "<mpls_tc>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_MPLS_TTL",
"value": "<mpls_ttl>"
}
]
},
{
"zero_or_one": [
{
"action": "DEC_MPLS_TTL"
}
]
},
{
"zero_or_one": [
{
"action": "OUTPUT",
"port": "<port_no>"
}
]
}
]
}
]
},
{
"zero_or_one":[
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_SRC",
"value": "<eth_src>"
}
]
},
{
```

```
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_DST",
"value": "<eth_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IPV4_SRC",
"value": "<ipv4_src>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IPV4_DST",
"value": "<ipv4_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IP_DSCP",
"value": "<ip_dscp>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "TCP_SRC",
"value": "<tp_src>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "TCP_DST",
"value": "<tp_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "UDP_SRC",
"value": "<tp_src>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "UDP_DST",
"value": "<tp_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_QUEUE",
"queue_id": "<queue_id>"
}
]
},
```

```
{
"zero_or_one": [
{
"action": "OUTPUT",
"port": "<port_no>"
},
{
"action": "OUTPUT",
"port": "<reserved_port>"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
},
{
"action": "GROUP",
"group_id": "L2 Rewrite"
},
{
"action": "GROUP",
"group_id": "ACL Multi-Output"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
}
]
}
]
}
]
},
{
"name": "IPv6 Mode",
"priority": "0..65535",
"doc": [
"IPv6 mode."
],
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "METADATA",
"value": "<metadata>",
"match_type": "mask"
},
{
"field": "ETH_DST",
"value": "<eth_dst>",
"match_type": "mask"
},
{
"field": "ETH_SRC",
"value": "<eth_src>",
"match_type": "mask"
},
{
"field": "ETH_TYPE",
"value": "<eth_type>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_PCP",
"value": "<vlan_pcp>",
"match_type": "all_or_exact"
},
{
"field": "IP_DSCP",
"value": "<ip_dscp>",
"match_type": "all_or_exact"
},
{
"field": "IP_PROTO",
"value": "<ip_proto>",
"match_type": "all_or_exact"
},
{
"field": "IPV6_SRC",
```

```
"value": "<ipv6_src>",
"match_type": "mask"
},
{
"field": "IPV6_DST",
"value": "<ipv6_dst>",
"match_type": "mask"
},
{
"field": "TCP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "TCP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "UDP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "UDP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "SCTP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "SCTP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "ICMPV6_TYPE",
"value": "<icmpv6_type>",
"match_type": "all_or_exact"
},
{
"field": "ICMPV6_CODE",
"value": "<icmpv6_code>",
"match_type": "all_or_exact"
},
{
"field": "INNER_VLAN_VID",
"value": "<inner_vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "INNER_VLAN_PCP",
"value": "<inner_vlan_pcp>",
"match_type": "all_or_exact"
}
],
"instruction_set": [
{
"zero_or_one": [
{
"instruction": "METER",
"meter_id": "<meter_id>"
}
]
},
{
"zero_or_one":[
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one": [
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_SRC",
"value": "<eth_src>"
}
]
```

```
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_DST",
"value": "<eth_dst>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IP_DSCP",
"value": "<ip_dscp>"
}
]
},
{
"zero_or_one": [
{
"action": "SET_QUEUE",
"queue_id": "<queue_id>"
}
]
},
{
"zero_or_one": [
{
"action": "OUTPUT",
"port": "<port_no>"
},
{
"action": "OUTPUT",
"port": "<reserved_port>"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
},
{
"action": "GROUP",
"group_id": "L2 Rewrite"
},
{
"action": "GROUP",
"group_id": "ACL Multi-Output"
},
{
"action": "GROUP",
"group_id": "L3 ECMP"
}
]
}
]
}
]
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"Default pass through, Policy ACL must forward or packet dropped."
],
"match_set": [],
"instruction_set": []
}
]
},
{
"name": "Egress_Port_Flow_Table",
"doc": [
"First table in egress pipeline, represent egress pipeline start.",
"No flow is allowed to add in this table."
```

```
],
"flow_mod_types": [],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Egress_Port_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Egress_Port_Group_Flow_Table"
}
]
}
]
},
{
"name": "Egress_Port_Group_Flow_Table",
"doc": [
"Match output port, table size is ports num + 1.",
"Output port egress Grouping."
],
"flow_mod_types": [
{
"name": "Egress Port Group",
"priority": "32768",
"doc": [
"Bundles multiple OpenFlow ports in a group."
],
"match_set": [
{
"field": "OUTPUT_PORT",
"value": "<port_no>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "WRITE_METADATA",
"metadata": "<metadata>",
"doc": [
"bit16-22: Port Group [0-127]"
]
},
{
"instruction": "GOTO_TABLE",
"table": "Egress_VLAN_Xlate_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Egress_Port_Group_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "WRITE_METADATA",
"metadata": "<metadata>",
"doc": [
"metadata: port_group = 0"
]
},
{
"instruction": "GOTO_TABLE",
"table": "Egress_VLAN_Xlate_Flow_Table"
}
]
}
]
},
{
"name": "Egress_VLAN_Xlate_Flow_Table",
"doc": [
"QinQ egress vlan xlate table for packets, table size is 4K."
],
"flow_mod_types": [
{
"name": "Egress VLAN Conversion",
```

```
"priority": "32768",
"doc": [
"This entry is for converting outgoing Tagged packets from QinQ to Single Tagged or untagged."
],
"match_set": [
{
"field": "METADATA",
"value": "<metadata>",
"match_type": "mask"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "exact"
},
{
"field": "INNER_VLAN_VID",
"value": "<inner_vlan_vid>",
"match_type": "exact"
}
],
"instruction_set": [
{
"instruction": "APPLY_ACTIONS",
"actions": [
{
"zero_or_one":[
{
"action": "POP_VLAN"
}
]
},
{
"zero_or_one":[
{
"action": "POP_VLAN"
}
]
},
{
"zero_or_one":[
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
}
]
}
]
},
{
"instruction": "GOTO_TABLE",
"table": "Egress_ACL_Flow_Table"
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default Table Miss",
"priority": "0",
"doc": [
"This entry cannot be updated or deleted because it is configured by switch chip hardware.",
"This is Switch Default Entry for Table-Miss in Egress_VLAN_Xlate_Flow_Table."
],
"match_set": [],
"instruction_set": [
{
"instruction": "GOTO_TABLE",
"table": "Egress_ACL_Flow_Table"
}
]
}
]
},
{
"name": "Egress_ACL_Flow_Table",
"doc": [
"Egress TCAM match on variety of fields.",
"Can drop, normal etc."
],
"flow_mod_types": [
{
"name": "IPv4 Mode",
"priority": "0..65535",
"doc": [
"IPv4 mode."
],
```

```
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "OUTPUT_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "ETH_DST",
"value": "<eth_dst>",
"match_type": "mask"
},
{
"field": "ETH_SRC",
"value": "<eth_src>",
"match_type": "mask"
},
{
"field": "ETH_TYPE",
"value": "<eth_type>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_PCP",
"value": "<vlan_pcp>",
"match_type": "all_or_exact"
},
{
"field": "IP_DSCP",
"value": "<ip_dscp>",
"match_type": "all_or_exact"
},
{
"field": "IP_PROTO",
"value": "<ip_proto>",
"match_type": "all_or_exact"
},
{
"field": "IPV4_SRC",
"value": "<ipv4_src>",
"match_type": "mask"
},
{
"field": "IPV4_DST",
"value": "<ipv4_dst>",
"match_type": "mask"
},
{
"field": "TCP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "TCP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "UDP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "UDP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "SCTP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "SCTP_DST",
"value": "<tp_dst>",
"match_type": "mask"
}
],
"instruction_set": [
```

```
{
"zero_or_one":[
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one":[
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IP_DSCP",
"value": "<ip_dscp>"
}
]
},
{
"zero_or_one": [
{
"action": "OUTPUT",
"port": "NORMAL"
}
]
}
]
}
]
}
]
},
{
"name": "IPv6 Mode",
"priority": "0..65535",
"doc": [
"IPv6 mode."
],
"match_set": [
{
"field": "IN_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "OUTPUT_PORT",
"value": "<port_no>",
"match_type": "all_or_exact"
},
{
"field": "ETH_DST",
"value": "<eth_dst>",
"match_type": "mask"
},
{
"field": "ETH_SRC",
"value": "<eth_src>",
"match_type": "mask"
},
{
"field": "ETH_TYPE",
"value": "<eth_type>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_VID",
"value": "<vlan_vid>",
"match_type": "all_or_exact"
},
{
"field": "VLAN_PCP",
"value": "<vlan_pcp>",
"match_type": "all_or_exact"
},
{
"field": "IP_DSCP",
"value": "<ip_dscp>",
"match_type": "all_or_exact"
},
{
"field": "IP_PROTO",
"value": "<ip_proto>",
"match_type": "all_or_exact"
},
{
```

```
"field": "IPV6_SRC",
"value": "<ipv6_src>",
"match_type": "mask"
},
{
"field": "IPV6_DST",
"value": "<ipv6_dst>",
"match_type": "mask"
},
{
"field": "TCP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "TCP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "UDP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "UDP_DST",
"value": "<tp_dst>",
"match_type": "mask"
},
{
"field": "SCTP_SRC",
"value": "<tp_src>",
"match_type": "mask"
},
{
"field": "SCTP_DST",
"value": "<tp_dst>",
"match_type": "mask"
}
],
"instruction_set": [
{
"zero_or_one":[
{
"instruction": "CLEAR_ACTIONS"
}
]
},
{
"zero_or_one":[
{
"instruction": "WRITE_ACTIONS",
"actions": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "IP_DSCP",
"value": "<ip_dscp>"
}
]
},
{
"zero_or_one": [
{
"action": "OUTPUT",
"port": "NORMAL"
}
]
}
]
}
]
}
]
}
],
"built_in_flow_mods": [
{
"name": "Default",
"priority": "0",
"doc": [
"Default pass through, Egress ACL must forward or packet dropped."
],
"match_set": [],
"instruction_set": []
}
]
```

```
}
],
"group_entry_types": [
{
"name": "L3 Fast Failover",
"doc": [
"Working (1) or backup (0) path bucket.",
"Both buckets for Routing",
"Watch OAM Protection Liveness Logical Port",
"Naming Convention: Type [31:28]:13, Index [27:0]:0xnnnnnn"
],
"group_type": "FAST_FAILOVER",
"bucket_types": [
{
"name": "Working (1)",
"action_set": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
}
],
"watch": "<port_no>"
},
{
"name": "Protection (0)",
"action_set": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
}
],
"watch": "<port_no>"
}
]
},
{
"name": "L3 ECMP",
"doc": [
"Used to specify IP multipath.",
"Naming Convention : Type [31:28]:7, Id [27:0]:0xnnnnnn"
],
"group_type": "SELECT",
"bucket_types": [
{
"name": "Multipath Destination",
"action_set": [
{
"at_least_one": [
{
"action": "GROUP",
"group_id": "L3 Unicast"
},
{
"action": "GROUP",
"group_id": "L3 Fast Failover"
}
]
}
]
}
]
},
{
"name": "ACL Multi-Output",
"doc": [
"Support Multi-Output by ACL Write-Action(Group(ALL))",
"Set-field actions must be consistent",
"Used by ACL only."
],
"group_type": "ALL",
"bucket_types": [
{
"name": "Multi-Output",
"action_set": [
{
"at_least_one": [
{
"action": "GROUP",
"group_id": "L2 Rewrite"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
}
]
}
]
}
```

```
]
},
{
"name": "L3 Multicast",
"doc": [
"Used for specify IP Replication.",
"VLAN id values must be consistent",
"Naming Convention : Type [31:28]:6, VLAN Id [27:16]:0xnnn, Id [15:0]:0xnnnn",
"Used by Multicast Routing only."
],
"group_type": "ALL",
"bucket_types": [
{
"name": "Replica",
"action_set": [
{
"at_least_one": [
{
"action": "GROUP",
"group_id": "L3 Multicast Interface"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
}
]
}
]
}
]
},
{
"name": "L3 Multicast Interface",
"doc": [
"Used for L3 multicast.",
"ALLOW_IN_PORT=1 by default.",
"VLAN Id must be consistent with interface group.",
"Naming Convention : Type [31:28]:5, Id [27:0]:0xnnnnnn"
],
"group_type": "INDIRECT",
"bucket_types": [
{
"name": "RewriteEthernetHeader",
"action_set": [
{
"action": "SET_FIELD",
"field": "ETH_SRC",
"value": "<eth_src>"
},
{
"action": "SET_FIELD",
"field": "VLAN_VID",
"value": "<vlan_vid>"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
}
]
}
]
},
{
"name": "L3 Unicast",
"doc": [
"Used for Ethernet next hop configuration.",
"ALLOW_IN_PORT=1 by default for this group.",
"Naming Convention : Type [31:28]:2, Id [27:0]:0xnnnnnn"
],
"group_type": "INDIRECT",
"bucket_types": [
{
"name": "RewriteEthernetHeader",
"action_set": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_SRC"
}
]
},
{
"action": "SET_FIELD",
"field": "ETH_DST"
},
{
"action": "SET_FIELD",
```

```
"field": "VLAN_VID"
},
{
"action": "GROUP",
"group_id": "L2 Interface"
}
]
}
]
},
{
"name": "L2 Rewrite",
"doc": [
"Used to modify Ethernet header fields for bridged packets.",
"Naming Convention : Type [31:28]:1, Id [27:0]:0xnnnnnn, :"
],
"group_type": "INDIRECT",
"bucket_types": [
{
"name": "RewriteEthernetHeader",
"action_set": [
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_SRC"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "ETH_DST"
}
]
},
{
"zero_or_one": [
{
"action": "SET_FIELD",
"field": "VLAN_VID"
}
]
},
{
"action": "GROUP",
"group_id": "L2 Interface"
}
]
}
]
},
{
"name": "L2 Interface",
"doc": [
"Port VLAN filtering enabled, this VLAN allowed.",
"Implementations can use to configure egress port VLAN.",
"Naming Convention : Type [31:28]:0, Vlan Id [27:16]:0xnnn, Port [15:0]:0xnnnn",
"NOTICE: POP_VLAN and set DSCP action do not support in L3 table."
],
"group_type": "INDIRECT",
"bucket_types": [
{
"name": "VlanTagging",
"action_set": [
{
"action": "OUTPUT",
"port": "<port_no>"
}
]
}
]
}
]
}
```

Configuring udf flow

Abstract

The goal is to be able to add flows which utilizes the udf (User defined filter) function of the hardware.

As hardware cannot parse the L3 protocol of an mpls packet, we can not match both mpls labels and transport layer ports. But we can do this by utilizing the udf function of hardware. The udf allow us to match 4 bytes of content at the given offset of the L2 header of the L3 header. The L2 header refers to the mac header of frame, and the L3 header refers to the first mpls lable of mpls frame or IP header of the non-mpls frame (in other words the header next to the inner VLAN tag).

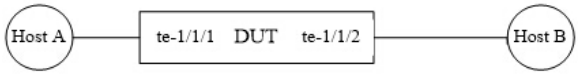
Due to the limitation of the hardware, we only support 4 fields of udf. The max number of udf flows share the same limitation of normal tcam flows.

> Note:
>
> Only untag packets can be matched when configure udf base L2 and L3 at the same time.

Example 1

Send IP packets with dl_dst 22:22:22:22:22:22, dl_src 22:11:11:11:11:11, tag 1000.

And we want to match this tag.



Step1: Create a new bridge named br0

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

Step 3: Configure udf and add flow

```
ovs-vsctl set-udf-mode "udf0(l2,offset=12,length=4)"
ovs-ofctl add-flow br0 table=250,in_port=1,udf0=0x810003E8/0x0000ffff,actions=2
```

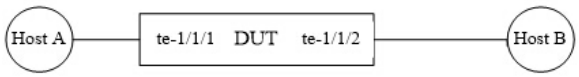
Step 4: Check table

```
admin@PicOS-OVS$ovs-vsctl show-udf-mode
  udf mode is udf0(l2,offset=12,length=4)
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br-vi
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=25.315s, table=250, n_packets=n/a, n_bytes=0, in_port=4,udf0=0x3e8/0xffff actions=output:5
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#1 udf permanent recirc_id=0,in_port=4,udf0=0x3e8/0xffff, actions:5
#0 normal permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
admin@PicOS-OVS$
```

Example 2

Send IP packets with dl_dst 22:22:22:22:22:22, dl_src 22:11:11:11:11:11,ip_src=192.168.200.100,ip_dst=192.168.100.100,tp_src=2002,tp_dst=3003,mpls_label=666;

And we want to match mpls_label and tp_src:



Step1: Create a new bridge named br0

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 2: Add ports to br0

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1  -- set Interface te-1/1/1 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1  -- set Interface te-1/1/2 type=pica8
```

Step 3: Configure udf and add flow

```
ovs-vsctl set-udf-mode "udf0(l3,offset=0,length=4), udf1(l3,offset=24,length=2)"
ovs-ofctl add-flow br0 table=250, in_port=1,udf0=0x0029a140/0xfffff000,udf1=0x07d2,actions=2
```

Note:

1. Offset needs to be aligned on 4 bytes and less than or equal to 124, length is less than or equal to 4.
2. (base, offset, length) defines one field of udf. Base refers to L2 or L3. Due to hardware limitations, we only support 4 fields of udf. But the max number of udf flows share the same limitation of normal tcam flows. L2 fields must be placed before L3 fields, and fields are in ascending order of offset with no overlapping of each other.
3. In the udf table, we can only use udf match format. We can not use both OXM (OpenFlow Extensible Match) and udf format in the same flow.
4. Flows in other tables can not use goto action with a udf table, and udf tables do not support goto action either, supporting output and drop actions,and from version 2.6.4,udf actions also support set_queue,meter and normal.
5. All udf flows will have higher priority than all the other tcam flows.
6. Adding udf flows will return errors, when there are arp or mpls flows in hardware already; also arp or mpls flows will return an error when there are udf flows in the hardware table already.
7. When adding udf flows, table=250 in match field is needed.
8. User cannot enable udf mode and match mode at the same time.

UDF L4

From PicOS2.8.0, picos support UDF offset from L4. The L4 header refers to L4 protocol ports, such as tcp or udp.

For example:

Send packets with：

dl_dst=22:22:22:22:22:22,dl_src=22:11:11:11:11:11, dl_vlan=199,nw_dst=1.1.1.1,nw_src=2.2.2.2,udp,udp_src=1234,udp_dst=5678

And we will match udp source port and destination port with udf.

Configure udf:

```
admin@PicOS-OVS$ovs-vsctl set-udf-mode "udf0(l4,offset=0,length=4)"
```

Add flow.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,table=250,udf0=0x04d2162e,actions=2
```

Macro UDF

From PicOS2.8.0, support a new format to add udf flow entry. Different from previous use (base, offset, length) to configure udf, user can use udf fields to configure it now.

1)Show all udf field.

```
admin@PicOS-OVS$ovs-vsctl show-udf-field
     Udf support fields:
    Match field                   layer       Offset      Length
    ------------------------------------------------------------
    dl_type                       l2          12          2
    vlan_inner                    l2          16          4
    mpls_outermost                l3          0           4
    ip_src                        l3          12          4
    ip_dst                        l3          16          4
    l2gre_key                     l3          24          4
    l2gre_ip_src_high             l3          52          4
    l2gre_ip_src_low_dst_high     l3          56          4
    l2gre_ip_dst_low              l3          60          2
    l2gre_ip_src_high_tag         l3          56          4
    l2gre_ip_src_low_dst_high_tag l3          60          4
    l2gre_ip_dst_low_tag          l3          64          2
```

```
    l4_port                      l4          0           4
    vxlan_vni                    l4          12          3
    vxlan_ip_src_high            l4          40          4
    vxlan_ip_src_low_dst_high    l4          44          4
    vxlan_ip_dst_low             l4          48          2
    vxlan_ip_src_high_tag        l4          44          4
    vxlan_ip_src_low_dst_high_tag l4         48          4
    vxlan_ip_dst_low_tag         l4          52          2
admin@PicOS-OVS$
```

2)configure macro udf.

```
admin@PicOS-OVS$ovs-vsctl set-macro-udf dl_type,ip_src,ip_dst
```

The match field can be any field in show-udf-field.

3)show udf mode.

```
admin@PicOS-OVS$ovs-vsctl show-udf-mode
```

or:

```
admin@PicOS-OVS$ovs-vsctl show-macro-udf
```

For example:

We will match vxlan vni for sending vxlan packets with vni=1122867.

1)Configure macro udf.

```
admin@PicOS-OVS$ovs-vsctl set-macro-udf vxlan_vni
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl show-udf-mode
  udf mode is udf0(l4,offset=12,length=3)
admin@PicOS-OVS$ovs-vsctl show-macro-udf
  macro udf mode is
 vxlan_vni : udf0(l4,offset=12,length=3)
admin@PicOS-OVS$
```

2)Add flow to macth vni.

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=250,udf0=0x112233,actions=3
```

1.l4 can not work with l2/l3.

2.If you want to configure l2 and l3 udf at the same time, the matched packets must be untag packets.

3.It cannot match the tag value which packets have one tag using macro udf.

UDF on TD3

Three commands you can use to show and set udf.

```
ovs-vsctl show-udf-base
ovs-vsctl show-udf-mode
ovs-vsctl set-udf-mode MODE
```

On trident3 platforms, using "ovs-vsctl show-udf-base" will show udf_v2 base types.

```
root@PICOS-OVS:~# ovs-vsctl show-udf-base
UDF_v2 base types:

 base-id    base-packet-format                                    description
 ----------------------------------------------------------------------------------------------------
 1          UdfAbstractPktFormatUnknownL3                 Abstract from the start of first byte after unknown ethertype.
 2          UdfAbstractPktFormatKnownNonIp                Abstract from the start of first byte after Known non-ip ethertype (other than Known IPv4/6 and FcoE/Mim/MPLS tunnels).
 3          UdfAbstractPktFormatKnownL3MplsOneLabel       Abstract from the start of MPLS Header with one label.
```

4	UdfAbstractPktFormatKnownL3MplsTwoLabel	Abstract from the start of MPLS Header with two labels.
5	UdfAbstractPktFormatUnknownL4	Abstract from the start of first byte of unknown L4 Header.
6	UdfAbstractPktFormatUdpUnknownL5	Abstract from the start of first byte of unknown L5 after UDP Header.
7	UdfAbstractPktFormatUdpVxlan	Abstract from the start of first byte of known L5 VXLAN header after UDP.
8	UdfAbstractPktFormatTcpUnknownL5	Abstract from the start of first byte of TCP.
9	UdfAbstractPktFormatGreWithoutKey	Abstract from the start of first byte of L4 header for GRE packets without key flag set (C=0/1, R=0/1 and K=0).
10	UdfAbstractPktFormatGreWithKey	Abstract from the start of first byte of L4 header for GRE packet

Users can set udf mode using command **"ovs-vsctl set-udf-mode "udf0(base=2,offset=0,length=2)"",**on td3 support 10 base ids. According to above descriptions of each base id to set the udf mode you need.

Match standard head in UDf mode

Prior to this, UDF match format can not mix with other OXM(OpenFlow Extensible Match) except for in_port in a flow. Now we remove the restriction from version 3.2. In UDF mode, we can use both UDF format and other standard header fields which are defined by OpenFlow as matching fields in the same flow.All the standard match fields in flows can be used with udf fields except for "ipv6_src, ipv6_dst, ipv6_label, mpls_label, mpls_label2, arp_op, arp_tpa, arp_spa, vn_tag, ingress_lag, tcp_flags, inner_vlan_vid and inner_vlan_pcp".

Note

- UDF match can only be used in Table 250 for flows.
- UDF flows have conflict witch arp and mpls flows which can not appear in hardware together
- Flows mixing standard match fields with UDF format have no influence on the capacity of UDF flows.
- UDF flows have the higher priority than normal flows because the group priority of UDF flows' is 1 while normal flow's is 0.
- In match mode, we add a new match mode **"udf_ext_ipv4"** to distinguish it from the old "udf" match mode. The available standard match fields for "udf_ext_ipv4" mode are the same to the normal UDF mode.
- All platforms except for TD(trident) support mixed UDF with more standard match fields in the same flow.

Non-match-mode

enable udf mode

```
ovs-vsctl set-udf-mode "udf0(l2,offset=12,length=4)"
```

add flow

```
ovs-ofctl add-flow br0 table=250,in_port=1,dl_dst=00:11:11:11:11:11,dl_src=00:22:22:22:22:22,dl_vlan=100,udf0=0x81(
```

Match-mode

In match mode,you must use "udf_ext_ipv4" group if you want to use udf and standard fields at the same time.And "udf_ext_ipv4" group also works well with other match mode groups.

set match mode and enable udf mode

```
ovs-vsctl set-match-mode udf_ext_ipv4=2000-3000
ovs-vsctl set-udf-mode "udf0(l2,offset=12,length=4)"
```

add flow

```
ovs-ofctl add-flow br0 table=250,in_port=1,priority=2000,dl_dst=00:11:11:11:11:11,dl_src=00:22:22:22:22:22,udf0=0x8
```

Goto_table

PicOS OVS supports goto_table on all platforms. When user dump-tables, tables 0 to 253 can be seen, but PicOS OVS only supports table 0. Also, flows will be merged as a flow to hardware when configuring flows with different tables.

Example 1. add flow entries with one goto action.

1) Add bridge

```
admin@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

2) Add ports to br0

```
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/13 vlan_mode=trunk tag=1 -- set interface ge-1/1/13 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/15 vlan_mode=trunk tag=1 -- set interface ge-1/1/15 type=pica8
admin@PicOS-OVS$ovs-vsctl add-port br0 ge-1/1/17 vlan_mode=trunk tag=1 -- set interface ge-1/1/17 type=pica8
```

3) Add flows with actions=goto_table:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=200,in_port=13,actions=goto_table:1
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=1,priority=101,in_port=13,ip,nw_src=10.10.10.11,actions=15
```

After adding flows, check software table and hardware table:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=10, cookie=0x0, duration=18.552s, table=0, n_packets=n/a, n_bytes=0, priority=200,in_port=13 actions=goto_
 flow_id=11, cookie=0x0, duration=4.648s, table=1, n_packets=n/a, n_bytes=0, priority=101,ip,in_port=13,nw_src=10.1
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#3 normal permanent flow_id=10 priority=200,ip,in_port=13,nw_src=10.10.10.11, actions:15
#0 normal_d permanent flow_id=2 priority=0, actions:drop
Total 2 flows in HW.
```

From the example above, two flow entries were merged as one flow entry in the hardware table, and we only use table=0. The priority of flow entry in hardware is decided by flow in table=0.

Example 2. add flow entries with two goto action.

Add flows:

```
admin@PicOS-OVS$ovs-ofctl add-flow br0 priority=200,in_port=13,actions=goto_table:1
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=1,priority=101,in_port=13,ip,nw_src=10.10.10.11,actions=15
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=1,priority=102,ip,nw_src=10.10.10.12,actions=goto_table:2
admin@PicOS-OVS$ovs-ofctl add-flow br0 table=2,priority=123,dl_dst=00:11:22:33:44:55,actions=17
admin@PicOS-OVS$
```

After adding flows, check software table and hardware table:

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=6, cookie=0x0, duration=43.530s, table=0, n_packets=n/a, n_bytes=0, priority=200,in_port=13 actions=goto_t
 flow_id=8, cookie=0x0, duration=15.120s, table=1, n_packets=n/a, n_bytes=0, priority=102,ip,nw_src=10.10.10.12 act
 flow_id=7, cookie=0x0, duration=25.110s, table=1, n_packets=n/a, n_bytes=0, priority=101,ip,in_port=13,nw_src=10.1
 flow_id=9, cookie=0x0, duration=4.330s, table=2, n_packets=n/a, n_bytes=0, priority=123,dl_dst=00:11:22:33:44:55 a
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#1 normal permanent flow_id=6 priority=200,ip,in_port=13,nw_src=10.10.10.11, actions:15
#2 normal permanent flow_id=6 priority=201,ip,in_port=13,dl_dst=00:11:22:33:44:55,nw_src=10.10.10.12, actions:17
Total 3 flows in HW.
admin@PicOS-OVS$
```

This example shows that four flow entries in table0 and table1 have goto action, so these flows are merged as two flows in hardware.

Optimizing TCAM Usage

- Configuring extend-group
- Configuring match-mode

Configuring extend-group

TCAM flow table support add arp/mpls and other normal flows. Due to ASIC limitation these flows cannot use one same slice, so we use group to devide these flows. In other words, arp and mpls flows use different groups from normal flow, we said them extend groups.

Before PicOS2.8.1, user can add these different groups flow at same time. From PicOS2.8.1, user also can add these flows at same time, but also can control disable or enable extend group for arp/mpls flows. The command as below,

ovs-vsctl disable-extend-group <TRUE|FALSE>

Once disable it, user will not allowed to add arp flow which include arp_tpa or arp_spa, and not allowed to add mpls flow include mpls_label. But support add dl_type=0x0806 and dl_type=0x8847/0x8848.

For example,

```
admin@PicOS-OVS$ovs-vsctl disable-extend-group TRUE
  Please reboot for the change to take effect!
admin@PicOS-OVS$sudo systemctl restart picos

.........................
admin@PicOS-OVS$ovs-pica8 entered promiscuous mode
device br0 entered promiscuous mode
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl show-extend-group
extend group: disabled
admin@PicOS-OVS$
```

Configuring match-mode

By default, 2 TCAM entries are used to support all matching tuples for all flows even if the flow does not use all matching tuples. All the groups below can be used in combination.

PicOS allows users to configure the switch in short flow TCAM match mode to optimize the TCAM usage, in this mode, each flow will only consume 1 TCAM entry (doubling the flows capacity in the TCAM).

When this mode is enabled (with the set-match-mode command), only specific fields can be used in the priority range defined by the command.Use " ovs-appctl pica /show tables" to check the max flows numbers can be installed to switch .

From version 2.11,pica8 switch support thirteen match mode groups.

The flows must use the exact fields described below:

mac(in_port: INGRESS_PORTS+INGRESS_LAG**):** ***"in_port,dl_src,dl_dst,dl_vlan,dl_type"***

mac_x(in_port: INGRESS_PORTS)**:** ***"in_port,dl_src,dl_dst,dl_vlan,dl_type"***

ip(in_port: INGRESS_PORTS+INGRESS_LAG)***: "in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800"***

ip_x(in_port: INGRESS_PORTS): ***"in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800"***

ipv4_quintuple(in_port: INGRESS_PORTS, dl_type: NONE): ***"in_port,dl_vlan,nw_src,nw_dst,tp_src,tp_dst,nw_proto,dl_type=0x0800"***

arp_tpa: ***"in_port,arp_tpa,dl_type=0x0806"***

arp_full: ***"in_port,dl_src,dl_dst,dl_vlan,arp_spa,arp_tpa,arp_op,dl_type=0x0806"***

arp_min: ***"in_port,arp_spa,arp_tpa,arp_op,dl_type=0x0806"***

l2l4: ***"in_port,dl_src,dl_dst,dl_vlan,dl_vlan_pcp,dl_type,nw_proto,nw_src,nw_dst,nw_tos,tp_src,tp_dst"***

ipv6_full:*"in_port,dl_vlan,ipv6_src,ipv6_dst,ipv6_label,tp_src,tp_dst,nw_proto,dl_type=0x86dd"* (from PicOS3.2.0, support ipv6_label in this group)

ipv6_src:*"in_port,dl_src,dl_dst,dl_vlan,ipv6_src,ipv6_label,nw_proto,dl_type=0x86dd"* (from PicOS3.2.0, support ipv6_label in this group)

ipv6_dst:*"in_port,dl_src,dl_dst,dl_vlan,ipv6_dst,ipv6_label,nw_proto,dl_type=0x86dd"* (from PicOS3.2.0, support ipv6_label in this group)

udf ***"in_port,udf0,udf1,udf2,udf3"***

You can use one or more fields in a match mode group.For example, if mac mode is enabled, all the flows must only use one or more fields defined in the mac mode. If mac and ip modes are enabled, then user can configure either mac flows or ip flows based on the fields described above. However, user cannot mixed the fields from mac and ip (that is, dl_src and nw_src).

Each match mode group is configured with a priority range. All the priorities can not be overlapped among all the match mode groups you configured.The max match mode groups you can configure in command "ovs-vsctl set-match-mode" must be not more than 10.

in the example below, all the flows between priority "10 and 1000" have to be Mac flows. All flows between 2000 and 20000 have to be IP flows and all flows between 30000 and 60000 have to be ARP flows, all flows between 50000 and 50001 have to be ipv6_full, all flows between 50002 and 50003 have to be ipv6_dst, all flows between 50004 and 60000 have to be ipv6_src.

1. all platforms support all the match mode groups from 2.11.
2. **all the vcap flows include l2gre encapsulation,vxlan encapsulation,push_pbb can not be supported.**
3. mac_x,ip_x,ipv4_quintuple match modes can not **match lag in port**.
4. udf mode is conflict with the arp match group.After enable udf mode,arp flow in arp match group can not be installed to flow table.
5. .ipv6 match mode group do not support vcap actions (eg:push_vlan,push_pbb)
6. The max flows of each match mode group has nothing to do with the numbers of match fields in a flow,but the width of the group ifself.
7. in tomahawk switch, nw_src or nw_dst is must added in ipv4_quintuple group.

From version 3.5,on trident3 chip' switches such as as7326_54x,add one command to enlarge max flow entries under match mode.The command and usage are as below:

command

ovs-vsctl disable-match-mode-inports TRUE|FALSE

true:do not enlarge the flow entries.

false:enlarge the flow entries

ovs-vsctl show-match-mode-inports

check the match-mode inports' status.

Test steps

step1:configure match mode

ovs-vsctl set-match-mode mac=1-100,mac_x=101-200 ...

step2:configure match-mode-inports

ovs-vsctl disable-match-mode-inports false

step3:add max flows in each match mode:

ovs-appctl pica/show tables

when "ovs-vsctl disable-match-mode-inports false",the max flow entries are as following:

match-mode	enable-inports(default)	disable-inports
mac	Double(3072)	IntraSliceDouble(9216)
mac_x	Double(3072)	IntraSliceDouble(9216)
ip	Double(3072)	IntraSliceDouble(9216)
ip_x	Double(3072)	IntraSliceDouble(9216)
ipv4_quintuple	Double(3072)	IntraSliceDouble(9216)
l2l4	Triple(3072)	Double(3072)
ipv6_full	Triple(3072)	Triple(3072)
ipv6_src	Triple(3072)	Double(3072)
ipv6_dst	Triple(3072)	Double(3072)
arp_tpa	IntraSliceDouble(9216)	IntraSliceDouble(9216)
arp_min	Double(3072)	IntraSliceDouble(9216)
arp_full	Double(3072)	Double(3072)
udf	IntraSliceDouble(9216)/Double(3072)	IntraSliceDouble(3072)
udf_ext_ipv4	Triple(3072)	Double(3072)/Triple(3072)

Examples

example1:arp_min group

Step1,set match mode to arp_min

```
ovs-vsctl set-match-mode arp_min=1-2000
```

Step2,add a flow

```
ovs-ofctl del-flows br0
ovs-ofctl add-flow br0 priority=1000,in_port=1,arp_spa=192.168.1.100,arp_tpa=192.168.2.100,arp_op=2,dl_type=0x0806,
ovs-appctl pica/dump-flows
```

Step3,send packets to te-1/1/1

a.Send arp packets with arp_spa is 192.168.1.100,arp tpa is 192.168.2.100,arp op is 2 to te-1/1/1

result:te-1/1/2 will transmit the arp packets.

b.Send arp packets with arp_spa is 192.168.1.100,arp tpa is 192.168.2.100,arp op is 1 to te-1/1/1

result:te-1/1/2 will not transmit the arp packets.

example2:l2l4 group

Step1,set match mode to l2l4 group

```
ovs-vsctl set-match-mode l2l4=1000-20000
```

Step2,add a flow with all match fields

```
ovs-ofctl del-flows br0
ovs-ofctl add-flow br0 priority=10000,in_port=1,vn_tag=0x01110222,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22
ovs-appctl pica/dump-flows
```

Step3,send packets to te-1/1/1

a.Send ip packets with vntag ethertype is 0x893f,vn_tag is 0x01110222,src mac is 22:11:11:11:11:11,dst mac is 22:22:22:22:22:22,dl_vlan=10,src ip is 192.168.1.100,dst ip is 192.168.2.100,vlan pcp is 3,nw_proto is 6,tos is 24,tp_src is 0x1000,tp_dst is 0x2000 to te-1/1/1.

result:te-1/1/2 will transmit the packets.

example3:udf match group

step1,set udf match mode

```
ovs-vsctl set-match-mode udf=2000-3000
```

step2,set udf mode

```
ovs-vsctl set-udf-mode "udf0(l2,offset=12,length=2)"
```

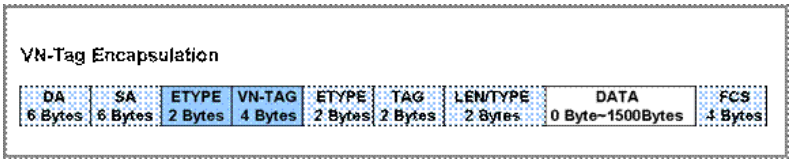
step3,add ipv4 flow with other priority except 2000-3000

```
ovs-ofctl add-flow br0 priority=500,table=250,in_port=1,udf0=0x0800,actions=14
```

VN-tag

From version 2.11,pica8 switch support vn-tag.This is a standard reported by VMware and Cisco,is a private technology of Cisco.Vn-tag is a tag before vlan in packets.Pica8 switch only support matching vn-tag and hashing by vn-tag.

1.packets format



16bits 1 1 14bits 1 1 2 12bits

| Ethertype | D | P | Dst_VIF | L | R | VER | Src_VIF |

---

2. detail description

Ethertype:pica8 switch can recognize two kinds of vn-tag packets with ethertype **0x8926 and 0x893f.**0x893f is the default ethertype of vn-tag packets switch can recognize.You can use command "ovs-vsctl set-vntag-ethertype **0x8926**" to set recognize another type of vn-tag packets.And use "ovs-vsctl show-vntag-ethertype" to show the current ethertype.

D|P ,L|R :can be 0 or 1,do not do any limitations.

Dst_vif:destination virtual interface.Can be any values.

Src_vif:source virtual interface.Can be any values.

3.matching vn-tag

Now support matching vn-tag in icap and udf table.Not support matching vn-tag in egress table.Examples as below.

```
admin@PICOS-OVS:~$ovs-vsctl set-vntag-ethertype 0x8926
admin@PICOS-OVS:~$ovs-ofctl del-flows br0
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 vn_tag=0x33330000/0x3FFF0000,dl_dst=00:11:11:11:11:11,actions=2
Send packets with vntag 0x8926,dst mac is 00:11:11:11:11:11,vntag is 0x33330000 to te-1/1/1.te-1/1/2 will transmit
```

4.hashing according to dst_vif and src_vif

For pica8 switch,support dst_vif and src_vif hash fields in ecmp/lag advance hash mapping fields,For a lag port,only support dst_vif|src_vif hash fields in advance mode.Also support these two fields in **l3-ecmp-select-group** and **lag-advance-hash-mapping-fields**.By default,src_vif and dst_vif is disabled in the hash fields.Examples as below:

example1:

step1. set ethertype for VN-tag

```
admin@PICOS-OVS:~$ovs-vsctl set-vntag-ethertype 0x8926
admin@PICOS-OVS:~$ovs-vsctl show-vntag-ethertype
```

step2.add a ecmp select group

```
admin@PICOS-OVS:~$ovs-vsctl set-group-ranges ecmp-select-groups=1-200
admin@PICOS-OVS:~$sudo systemctl restart picos
admin@PICOS-OVS:~$ovs-ofctl add-group br0 group_id=20,type=select,bucket=set_field:44:44:44:11:11:11-\>dl_src,outpu
```

step3. add a flow only matching dvif

```
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 vn_tag=0x01110000/0x3FFF0000,dl_dst=00:11:11:11:11:11,actions=group:20
admin@PICOS-OVS:~$ovs-ofctl dump-flows br0
admin@PICOS-OVS:~$ovs-appctl pica/dump-flows
```

step4.set ecmp hash field to svif

```
admin@PICOS-OVS:~$ovs-vsctl set-l3-ecmp-hash-fields src_vif
```

step5.send packets with vn-tag

Send 10000 vntag packets dst mac is 00:11:11:11:11:11,dvif is 0x0111,vntag ethertype is 8926,svif is changing,initial value is 001,changing 100
result:the packets will hash to the te-1/1/2 and te-1/1/3.te-1/1/2 will transmit the vntag packets with dst mac is switch mac,src mac is 44:44:44:11:11:11,te-1/1/3 will transmit the vntag packets with dst mac is switch mac,src mac is 66:66:66:11:11:11.

example2:

step1. set ethertype for VN-tag

```
admin@PICOS-OVS:~$ovs-vsctl set-vntag-ethertype 0x8926
admin@PICOS-OVS:~$ovs-vsctl show-vntag-ethertype
```

step2.add a lag select group

```
admin@PICOS-OVS:~$ovs-vsctl set-group-ranges lag-select-groups=201-300
admin@PICOS-OVS:~$sudo systemctl restart picos
admin@PICOS-OVS:~$ovs-ofctl add-group br0 group_id=220,type=select,bucket=set_field:44:44:44:11:11:11-\>dl_src,outp
```

step3. add a flow only matching dvif

```
admin@PICOS-OVS:~$ovs-ofctl del-flows br0
admin@PICOS-OVS:~$ovs-ofctl add-flow br0 vn_tag=0x01110000/0x3FFF0000,dl_dst=22:11:11:11:11:11,actions=group:220
admin@PICOS-OVS:~$ovs-ofctl dump-flows br0
admin@PICOS-OVS:~$ovs-appctl pica/dump-flows
```

step4.set ecmp hash field to svif

```
admin@PICOS-OVS:~$ovs-vsctl set-lag-advance-hash-mapping-fields src_vif
```

step5.send packets with vn-tag

Send 10000 vntag packets dst mac is 22:11:11:11:11:11,dvif is 0x0111,vntag ethertype is 8926,svif is changing,initial value is 001,changing 10

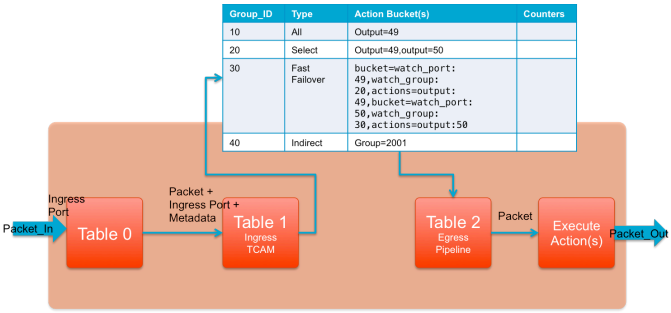
result:the packets will hash to the te-1/1/2 and te-1/1/3.te-1/1/2 and te-1/1/3 will transmit the vntag packets with dst mac is 22:11:11:11:11:11,src mac is 44:44:44:11:11:11.

Configuring Group

Creating a Group Table

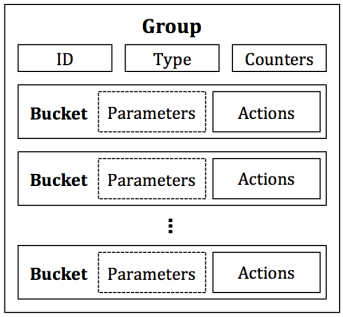
Group Tables

Group tables enable Openflow to process forwarding decisions on multiple links. Examples include: load-balancing, multicast, and active/standby.



The above figure illustrates how group-tables can simplify the configuration required to consolidate forwarding decisions for flows in an Openflow pipeline.

An **OpenFlow group** is an abstraction that facilitates more complex and specialized packet operations that cannot easily be performed through a flow table entry. Each group receives packets as input, and performs any OpenFlow actions on these packets. A group is not capable of performing any OpenFlow instructions, so it cannot send packets to other flow tables or meters. Furthermore, it is expected that packets have been matched appropriately prior to entry to a group, as groups do not support matching on packets. Groups are merely mechanisms to perform advanced actions, or sets of actions.



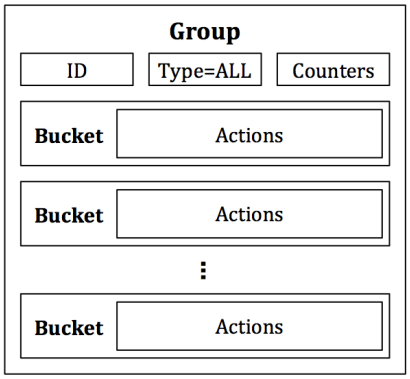
As shown in the above figure, the power of a group is that it contains separate lists of actions, and each individual action list is referred to as an **OpenFlow bucket**. Thus, it is said that a group contains a bucket list (or a list of lists of actions). Each bucket or list of buckets can be applied to entering packets; the exact behavior depends on the group type. There are certain types of groups that make use of additional parameters within a bucket. The details of these parameters will be discussed with each group type, where applicable.

There are four types of groups: **ALL**, **SELECT**, **INDIRECT**, and **FAST-FAILOVER**.

1. PicOS OVS supports group tables in Openflow 1.2 Openflow 1.3 and Openflow 1.4
2. The number of buckets supported is dependent on the TCAM size in the ASIC. So there is a possibility that all defined group tables will not be installed in hardware.
3. Max group number is 512, and max bucket number in one group is 128.

The ALL Group

Starting with one of the simplest, the **ALL group**, illustrated in the following figure, will take any packet received as input, and duplicate it to be operated on independently by each bucket in the bucket list. In this way, an ALL group can be used to replicate and then operate on separate copies of the packet defined by the actions in each bucket. Different and distinct actions can be in each bucket, which allows different operations to be performed on different copies of the packet.



Limitation in PicOS switch:

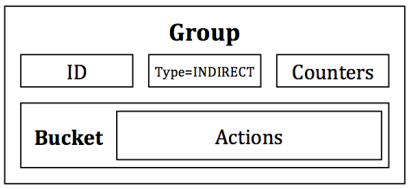
Due to limitation in the ASIC, PicOS OVS switches do not support replicating the packet and then operating by the actions in each bucket. So if user wants to configure type=all group, the actions of different buckets must be same. In other word, all the buckets need be uniform.

Example:

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=20,type=all,bucket=mod_dl_src=00:00:00:11:11:11,mod_dl_dst=22:22:2
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22:00:00:00:00:00,dl_type=0x0800

admin@PicOS-OVS$ovs-ofctl dump-groups br0 20
OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
 group_id=20,type=all,bucket=actions=set_field:00:00:00:11:11:11->eth_src,set_field:22:22:22:00:00:00->eth_dst,outp

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#134 normal permanent recirc_id=0,tcp,in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22:00:00:00:00:00,nw_src=1.1.2.10(
```

The INDIRECT Group

The **INDIRECT group** illustrated in the figure below, can be difficult to comprehend as a “group,” since it contains only a single bucket, where all packets received by the group are sent to this lone bucket. In other words, the INDIRECT group does not contain a list of buckets but a single bucket (or single list of actions) instead. The purpose of the INDIRECT group is to encapsulate a common set of actions used by many flows. For example, if flows A, B, and C match on different packet headers but have a common set or subset of actions, these flows can send packets to the single INDIRECT group as opposed to having to duplicate the list of common actions for each flow. The INDIRECT group is used to simplify an OpenFlow deployment and reduce the memory footprint of a set of similar flows.




```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=30,type=indirect,bucket=mod_dl_src=00:00:00:11:11:11,mod_dl_dst=22
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22:00:00:00:00:00,dl_type=0x0800
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_src=22:11:11:11:11:22,dl_dst=22:00:00:00:00:00,dl_type=0x0800

admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=7.342s, table=0, n_packets=n/a, n_bytes=0, tcp,in_port=11,dl_src=22:11:11:11:11:22,dl_dst=22
 cookie=0x0, duration=31.446s, table=0, n_packets=n/a, n_bytes=0, tcp,in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#136 normal permanent recirc_id=0,tcp,in_port=11,dl_src=22:11:11:11:11:22,dl_dst=22:00:00:00:00:00,nw_src=1.1.2.20(
#135 normal permanent recirc_id=0,tcp,in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22:00:00:00:00:00,nw_src=1.1.2.10(
```

The FAST-FAILOVER Group

Lastly, the **FAST-FAILOVER group** is the topic of conversation for this tutorial and is designed specifically to detect and overcome port failures. Like the SELECT and ALL groups, the FAST-FAILOVER group, as indicated in **Figure 5**, has a list of buckets. In addition to this list of actions, each bucket has a **watch port** and/or **watch group** as a special parameter. The watch port/group will monitor the “liveness” or up/down status of the indicated port/group. If the status is deemed to be down, then the bucket will not be used. If it is determined to be up, then the bucket can be used. Only one bucket can be used at a time, and the bucket in use will not be changed unless the status of the watch port/group transitions from up to down. When such an event occurs, the FAST-FAILOVER group will quickly select the next bucket in the bucket list with a watch port/group that is up.

Actually, watch group is not supported in PicOS.

There is no guarantee on the transition time to select a new bucket when a failure occurs. The transition time is dependent on search time to find a watch port/group that is up and on the switch implementation. However, the motivation behind using a FAST-FAILOVER group is that it is almost guaranteed to be quicker than consulting the control plane to handle the port down event, and inserting a new flow or set of flows. With FAST-FAILOVER groups, link failure detection and recovery takes place entirely in the data plane.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=fast_failover,bucket=watch_port:1,output:1
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=2,type=fast_failover,bucket=watch_port:2,output:2
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=3,type=fast_failover,bucket=watch_port:3,watch_group:1,output:5,bu

admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_src=22:11:11:11:11:11,dl_dst=22:00:00:00:00:00,dl_type=0x0800
```

The SELECT Group

Next, there is the **SELECT group**, which is primarily designed for load balancing. As indicated in the following figure, each bucket in a SELECT group has an assigned weight, and each packet that enters the group is sent to a single bucket. The bucket selection algorithm is undefined and is dependent on the switch's implementation; however, weighted round robin is perhaps the most obvious and simplest choice of packet distribution to buckets. The weight of a bucket is provided as a special parameter to each bucket. Each bucket in a SELECT group is still a list of actions, so any actions supported by OpenFlow can be used in each bucket, and the buckets need not be uniform.

> ⚠ PicOS does **not** support weight. Because OVS forward is based on priority of entries in TCAM, the traditional ECMP in routing table cannot be used. For a typical IP flow, PicOS implements a "dummy ECMP" by splitting the matching fields of a flow. For a group-table with type=select, PicOS support set-select-group-hash-fields and the packets will hash according to the value of set-select-group-hash-fields.

The command added for setting select-group hash fields is:

```
ovs-vsctl set-select-group-hash-fields [FIELDS]
FIELDS: default or some of [nw_src, nw_dst, dl_src, dl_dst] spliced by ",".

In the default mode the order is "nw_src, nw_dst, dl_src, dl_dst", so will check the first filed "nw_src" and find
```

Description: This command takes at most 1 argument that specifies match fields to do hash for select-group, these match fields should be spliced by "," with descending priority and must use the constrained fields list above. If there is 0 argument token or 1 argument with string "default", the default mode will take effect.

The priority for match fields means that when match fields are set, they will be checked in sequence to select one can do hash. If select fails, the first field in the configured match fields will be picked on and only one bucket can be used.

In default mode, the check order is "nw_src, nw_dst, dl_src, dl_dst" with non-zero field mask. If select failed, check the order "nw_src, nw_dst, dl_src, dl_dst" with field mask equals zero again.

If the selected field is an exact value, means all mask bits are "1", then only one bucket can be used.

> ⚠
>
> "When user want the traffic match nw_src or nw_dst to hash, the flow entry match field must include dl_type=0x0800. If not include dl_type=0x0800, the flow entry only hash by dl_src and dl_dst.ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=output:2"

Example

```
1. If the match field does not include dl_type=0x0800.

set-select-group-hash-fields: dl_src,dl_dst
admin@PicOS-OVS$ovs-vsctl set-select-group-hash-fields dl_src,dl_dst
admin@PicOS-OVS$ovs-vsctl show-select-group-hash-fields
select_group_hash_fields: dl_src,dl_dst

1> There is no dl_src or dl_dst in flow match field, use dl_src for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#4 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:01/00:00:00:00:00:03, actions:25
#5 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:00/00:00:00:00:00:03, actions:14
#2 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:03/00:00:00:00:00:03, actions:14
#3 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:02/00:00:00:00:00:03, actions:38

2> dl_src has hashable mask in flow match field, use dl_src for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:00:00:00/ff:ff:ff:00:00:00,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#9 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:00:00:00/ff:ff:ff:00:00:03, actions:14
#8 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:00:00:01/ff:ff:ff:00:00:03, actions:25
#7 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:00:00:02/ff:ff:ff:00:00:03, actions:38
#6 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:00:00:03/ff:ff:ff:00:00:03, actions:14

3> dl_src has no hashable mask and there is no dl_dst in flow match field, use dl_dst for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#13 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:11:11:11,dl_dst=00:00:00:00:00:00/00:00:00:00:00:03, ac
#12 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:11:11:11,dl_dst=00:00:00:00:00:01/00:00:00:00:00:03, ac
```

```
#11 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:11:11:11,dl_dst=00:00:00:00:00:02/00:00:00:00:00:03, ac
#10 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:11:11:11,dl_dst=00:00:00:00:00:03/00:00:00:00:00:03, ac

4> There is no dl_src, and dl_dst has hashable mask in flow match field, use dl_src for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:00:00:00/ff:ff:ff:00:00:00,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#83 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:01/00:00:00:00:00:03,dl_dst=22:22:22:00:00:00/ff:
#81 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:03/00:00:00:00:00:03,dl_dst=22:22:22:00:00:00/ff:
#84 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:00/00:00:00:00:00:03,dl_dst=22:22:22:00:00:00/ff:
#82 normal permanent recirc_id=0,in_port=1,dl_src=00:00:00:00:00:02/00:00:00:00:00:03,dl_dst=22:22:22:00:00:00/ff:

5> dl_src and dl_dst have no hashable mask in flow match field, won't hash,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#18 normal permanent recirc_id=0,in_port=1,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22, actions:14


2. If the match field include dl_type=0x0800.

set-select-group-hash-fields: nw_dst,nw_src,
admin@PicOS-OVS$ovs-vsctl set-select-group-hash-fields nw_dst,nw_src
admin@PicOS-OVS$ovs-vsctl show-select-group-hash-fields
select_group_hash_fields: nw_dst,nw_src

1> There is no nw_dst or nw_src in flow match field, use nw_dst for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#28 normal permanent recirc_id=0,ip,in_port=1,nw_dst=0.0.0.2/0.0.0.3, actions:38
#30 normal permanent recirc_id=0,ip,in_port=1,nw_dst=0.0.0.0/0.0.0.3, actions:14
#29 normal permanent recirc_id=0,ip,in_port=1,nw_dst=0.0.0.1/0.0.0.3, actions:25
#27 normal permanent recirc_id=0,ip,in_port=1,nw_dst=0.0.0.3/0.0.0.3, actions:14
2> nw_dst has hashable mask, use nw_dst for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_dst=192.168.2.0/24,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#35 normal permanent recirc_id=0,ip,in_port=1,nw_dst=192.168.2.3/255.255.255.3, actions:14
#37 normal permanent recirc_id=0,ip,in_port=1,nw_dst=192.168.2.1/255.255.255.3, actions:25
#38 normal permanent recirc_id=0,ip,in_port=1,nw_dst=192.168.2.0/255.255.255.3, actions:14
#36 normal permanent recirc_id=0,ip,in_port=1,nw_dst=192.168.2.2/255.255.255.3, actions:38

3> nw_dst has no hashable mask and there is no nw_src in match field, use nw_src for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_dst=192.168.2.100,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#40 normal permanent recirc_id=0,ip,in_port=1,nw_src=0.0.0.2/0.0.0.3,nw_dst=192.168.2.100, actions:38
#42 normal permanent recirc_id=0,ip,in_port=1,nw_src=0.0.0.0/0.0.0.3,nw_dst=192.168.2.100, actions:14
#41 normal permanent recirc_id=0,ip,in_port=1,nw_src=0.0.0.1/0.0.0.3,nw_dst=192.168.2.100, actions:25
#39 normal permanent recirc_id=0,ip,in_port=1,nw_src=0.0.0.3/0.0.0.3,nw_dst=192.168.2.100, actions:14

4> There is no nw_dst, and nw_src has hashable mask, use nw_dst for hashing,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=192.168.1.0/24,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#46 normal permanent recirc_id=0,ip,in_port=1,nw_src=192.168.1.0/24,nw_dst=0.0.0.1/0.0.0.3, actions:25
#44 normal permanent recirc_id=0,ip,in_port=1,nw_src=192.168.1.0/24,nw_dst=0.0.0.3/0.0.0.3, actions:14
#47 normal permanent recirc_id=0,ip,in_port=1,nw_src=192.168.1.0/24,nw_dst=0.0.0.0/0.0.0.3, actions:14
#45 normal permanent recirc_id=0,ip,in_port=1,nw_src=192.168.1.0/24,nw_dst=0.0.0.2/0.0.0.3, actions:38

5> nw_src and nw_dst have no hashable mask in match field, won't hash,
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:14,bucket=output:25,bucket=output:38
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=192.168.1.100,nw_dst=192.168.2.100,actions=
```

```
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#48 normal permanent recirc_id=0,ip,in_port=1,nw_src=192.168.1.100,nw_dst=192.168.2.100, actions:14


3. set-select-group-hash-fields: nw_src,dl_src

admin@PicOS-OVS$ovs-vsctl set-select-group-hash-fields nw_src,dl_src
admin@PicOS-OVS$ovs-vsctl show-select-group-hash-fields
select_group_hash_fields: nw_src,dl_src

admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:12,bucket=output:13,bucket=output:14
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,ip,nw_src=10.10.10.10,nw_dst=10.10.20.0/24,dl_src=00:00:00:11:11

The order is "nw_src, dl_src", so will check the first filed "nw_src" and find all mask bits of nw_src in flow entr
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#29 normal permanent recirc_id=0,ip,in_port=11,dl_src=00:00:00:11:11:00/ff:ff:ff:ff:ff:03,dl_dst=00:00:00:22:22:22
#27 normal permanent recirc_id=0,ip,in_port=11,dl_src=00:00:00:11:11:02/ff:ff:ff:ff:ff:03,dl_dst=00:00:00:22:22:22
#28 normal permanent recirc_id=0,ip,in_port=11,dl_src=00:00:00:11:11:01/ff:ff:ff:ff:ff:03,dl_dst=00:00:00:22:22:22
#26 normal permanent recirc_id=0,ip,in_port=11,dl_src=00:00:00:11:11:03/ff:ff:ff:ff:ff:03,dl_dst=00:00:00:22:22:22


4. set-select-group-hash-fields: nw_src,dl_dst
admin@PicOS-OVS$ovs-vsctl set-select-group-hash-fields nw_src,dl_dst
admin@PicOS-OVS$ovs-vsctl show-select-group-hash-fields
select_group_hash_fields: nw_src,dl_dst

admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:12,bucket=output:13,bucket=output:14
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,ip,nw_src=10.10.10.10,nw_dst=10.10.20.0/24,dl_src=00:00:00:11:11

The order is "nw_src, dl_dst", so will check the first filed "nw_src" and find all mask bits of nw_src in flow entr

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#30 normal permanent recirc_id=0,ip,in_port=11,dl_src=00:00:00:11:11:00/ff:ff:ff:ff:ff:00,dl_dst=00:00:00:22:22:22
```

Modify Bucket in a Group Table

The following configuration shows modification of buckets in a group table.

```
admin@PicOS-OVS# ovs-ofctl add-group br0 group_id=2238,type=all,bucket=output:3
admin@PicOS-OVS# ovs-ofctl mod-group br0 group_id=2238,type=all,bucket=output:2,bucket=output:3
admin@PicOS-OVS# ovs-ofctl mod-group br0 group_id=2238,type=all,bucket=mod_dl_src:22:11:11:22:22:22,mod_dl_dst:22:(
```

Delete Group Table

In following configuration, users can delete the group table with following CLI.

```
admin@PicOS-OVS$ovs-ofctl del-groups br0 group_id=2238
admin@PicOS-OVS$ovs-ofctl del-groups br0
```

Display the Information of Group Table

Users can display the information of all group tables.

```
admin@PicOS-OVS$ovs-ofctl dump-groups br0
OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
 group_id=20,type=all,bucket=actions=output:49
 group_id=30,type=all,bucket=actions=output:50
 group_id=10,type=ff,bucket=watch_port:49,watch_group:20,actions=output:49,bucket=watch_port:50,watch_group:30,act

admin@PicOS-OVS$ovs-ofctl dump-group-stats br0
OFPST_GROUP reply (OF1.4) (xid=0x2):
 group_id=20,duration=163370.539s,ref_count=0,packet_count=n/a,byte_count=0,bucket0:packet_count=n/a,byte_count=0
 group_id=30,duration=163365.129s,ref_count=0,packet_count=n/a,byte_count=0,bucket0:packet_count=n/a,byte_count=0 (
```

```
admin@PicOS-OVS$ovs-ofctl dump-group-features br0
OFPST_GROUP_FEATURES reply (OF1.4) (xid=0x2):
 Group table:
    Types:  0xf
    Capabilities:  0xe
    all group:
       max_groups=0x64
       actions: output group set_field strip_vlan push_vlan mod_nw_ttl dec_ttl set_mpls_ttl dec_mpls_ttl dec_mpls_t
    select group:
       max_groups=0x64
       actions: output group set_field strip_vlan push_vlan mod_nw_ttl dec_ttl set_mpls_ttl dec_mpls_ttl dec_mpls_t
    indirect group:
       max_groups=0x64
       actions: output group set_field strip_vlan push_vlan mod_nw_ttl dec_ttl set_mpls_ttl dec_mpls_ttl dec_mpls_t
    fast failover group:
       max_groups=0x64
       actions: output group set_field strip_vlan push_vlan mod_nw_ttl dec_ttl set_mpls_ttl dec_mpls_ttl dec_mpls_t
```

Ecmp Select Group

From PicOS 2.8.0, Pica8 switch supports the traffic which has processed in TCAM, still can hash as ecmp interface or lag interface.

In prior PicOS version, the traffic in TCAM table only could hash as select group, refer to chapter 'Creating a Group Table,' the hash algorithm is defined by the designer. But from the new version, user can use ecmp or lag to process traffic.

> 1, 'dec_ttl' only can be used in table=252 route table and ecmp-select-group, others will neglect it.
>
> Once configure ecmp-select-group, L2 table (table=251) cannot work.
>
> 2, Platforms P-3290/P-3295/P-3297 do not support configure ecmp-group.
>
> 3, The max ecmp group buckets number is 32.
>
> 4.When ecmp-select-group has been configured,the following functions cannot work.
>
> vxlan,gre,l2gre;
>
> push_pbb,pop_pbb;
>
> push_mpls,pop_mpls
>
> push_l2mpls,pop_l2mpls.

In default, ecmp and lag hash cannot work in TCAM table, user needs to use group table to define them. 'lag-select-groups=0-0' means the group ID range is 0-0, that is disable lag-select-groups. Same as others.

The command to show the ranges of ecmp-select-groups and lag-select-groups.

```
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges: default
  lag-select-groups=0-0
  ecmp-select-groups=0-0
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

ECMP Select Group

Select group uses ecmp, create an ecmp interface for each select group, and the ecmp interface contains egress interfaces which correspond to buckets in the group.

The command to configure ecmp-select-group ID range:

ovs-vsctl set-group-ranges ecmp-select-groups=<*min_value*>-<*max_value*>

The group IDs may be divided into different areas: ecmp-select-groups and the original groups. Ecmp-select-groups ranges is <*min_value*>-<*max_value*> and the rest of group IDs for original groups. The max range of group is 1-4294967039.

After configuring the command, user needs to reboot switch.

Use command **ovs-vsctl set-group-ranges** to back default group ranges.

```
admin@PicOS-OVS$ovs-vsctl set-group-ranges ecmp-select-groups=1-10000
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges:
  lag-select-groups=0-0
  ecmp-select-groups=1-10000
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

In ecmp select group can modify dl_dst, dl_src, dl_vlan, dec_ttl and set_queue. And the actions must be same in different buckets, the value can be the same or not.

If dec_ttl is set or set_field with vlan_vid,dl_src or dl_dst is set in an ecmp select group flow's actions, the ecmp will modify packet's corresponding field. If the fields are not set in an ecmp select group flow, the value also will be modified via L3 ecmp interface, and dl_src and dl_dst will be switch system mac and ttl will decrease.

User can use command 'set-l3-egress-keep-fields' to keep the field as original value.

ovs-vsctl set-l3-egress-keep-fields *[FIELDS]*

[FIELDS] allows one or more value of *{dl_vlan, dl_src, dl_dst, nw_ttl}.* If not special configure *[FIELDS]* , will back default value and the fields will be modified by L3 ecmp interface.

> During add flow entry whose actions include ecmp-select-group, other actions fields only support above fields: dl_src, dl_src, dl_vlan, dec_ttl and set_queue.

ovs-vsctl set-l3-ecmp-hash-fields *[FIELDS]*

<FIELDS> allowed values in_port, nw_dst, nw_proto, nw_src, port_dst, port_src, vlan, src_vif, dst_vif, gtp_teid. If not special configure <*FIELDS],* the default value is nw_src. If user want configure multiple values, should use blank.

```
admin@PicOS-OVS$ovs-vsctl set-l3-ecmp-hash-fields in_port nw_dst
```

Example 1

Set group 1 as an ecmp select group, modify dl_vlan, dl_src and dl_dst, dec ttl.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=set_field:10-\>vlan_vid,set_field:00:00:00:22
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,ip,actions=group:1

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#1 normal permanent flow_id=6 (ecmp select group) in_port=31, actions:egress_dec_ttl,set(eth(src=00:00:00:22:22:22
Total 2 flows in HW.
```

Example 2

Set group 1 as an ecmp select group, do not change dl_vlan,dl_src,dl_dst and ttl.

vlan_vid,dl_src and dl_dst are not set in an ecmp select group flow, and packet's corresponding fields stay unchanged.

```
admin@PicOS-OVS$ovs-vsctl set-l3-egress-keep-fields dl_vlan,dl_src,dl_dst,nw_ttl

admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:33,bucket=output:34
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,dl_vlan=30,dl_dst=00:00:00:11:11:11,actions=group:1

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#2 normal permanent flow_id=8 (ecmp select group) in_port=31,dl_vlan=30,dl_dst=00:00:00:11:11:11, actions:33,34
Total 2 flows in HW.
```

Example 3

Set group 1 as an ecmp select group, modify dl_vlan, dl_src only and other packet's corresponding fields stay unchanged.

```
admin@PicOS-OVS$ovs-vsctl set-l3-egress-keep-fields dl_dst,nw_ttl

admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=set_field:10-\>vlan_vid,set_field:00:00:00:22
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,actions=group:1

admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#3 normal permanent flow_id=9 (ecmp select group) in_port=31, actions:set(eth_src((src=00:00:00:22:22:22))),set_vla
Total 2 flows in HW.
```

LAG Select Group

LAG Select Group

If user wants the traffic load balance like lag interface and doesn't want special configuration lag interface, lag select group is one choice.

Select group uses lag, create an lag interface for each select group, and the lag interface contains egress interfaces which corresponds to buckets in the group.

> PICOS reserve ae1 to ae20 for static lag configuration, ae21 to ae48 use the internal lag for select group.
>
> PICOS will create internal lag when the user creates a lag select group. It only uses the first bucket actions except the output. It means that we can support 24 lag select groups.
>
> The physical port which has added in lag-select-group cannot be used in other groups and cannot work as one physical port.

Before add lag select group, user need configure group range.

The command to configure lag-select-group ID range:

ovs-vsctl set-group-ranges lag-select-groups=<*min_value*>-<*max_value*>

The group IDs may be divided into different areas: lag-select-groups and the original groups. Lag-select-groups ranges is <*min_value*>-<*max_value*> and the rest of group IDs for original groups. After configure the command, user needs to reboot switch.

```
admin@PicOS-OVS$ovs-vsctl set-group-ranges lag-select-groups=1-10000
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges:
  lag-select-groups=1-10000
  ecmp-select-groups=0-0
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

In lag select group can modify any fields switch support. And the actions must be configured in first bucket, other buckets only include output.

Example 1

Set group 1 as a lag select group, modify dl_vlan and dl_dst.

```
 admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=select,bucket=set_field:1000-\>vlan_vid,set_field:00:00:0(
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,actions=group:1
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#1 normal permanent flow_id=6 (lag select group) in_port=31, actions:set(eth_dst((dst=00:00:00:11:11:11))),set_vlar
Total 2 flows in HW.
```

Close all Group-ranges

If user want close the group-ranges, please use command as below.

ovs-vsctl set-group-ranges

```
admin@PicOS-OVS$ovs-vsctl set-group-ranges
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges:
  lag-select-groups=0-0
  ecmp-select-groups=0-0
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

Mirror Group

From PicOS 2.8.0, Pica8 switch support ingress-mirror-group and egress-mirror-group.

- Ingress-mirror-group: Packets can modify corresponding fields and send out from one port, at the same time the packets also can keep original and send out from other ports.
- Egress-mirror-group: Packets can modify corresponding fields send out from one port, also can send out from another port at same time.

Using configure type=all group to create ingress-mirror-group or egress-mirror-group.

- Ingress-mirror-group: Only support 2 buckets, the first bucket process packets as normal, use the second bucket to mirror original packets at ingress and send out from one physical port or lag interface.
- Egress-mirror-group: Only support 2 buckets, the first bucket process packets as normal, use the second bucket to mirror modified packets at egress and send out from one physical port or lag interface.

We said the output in second bucket as monitor port.

> 1. ingress/Egress mirror group only support configure 2 buckets; Monitor port can be physical port/lag port/lag-select-group.
>
> 2. lag-select-group can include multiple ports, but if lag-select-group as monitor port only first eight ports can work.
>
> 3. only support add 4 monitor port (include ingress+egress) at most.
>
> 4. ingress/egress mirror group only can configure in table=0 flow entry.
>
> 5. ingress/egress mirror group cannot configure dec_tll in bucket.
>
> 6.do not support any other actions except ingress/egress mirror group in a flow's action.All actions you want to use must be added to the first bucket of the ingress/egress mirror-group.

In default, ingress/egress-mirror-groups is disabled, user need use command to configure them. 'ingress-mirror-groups=0-0' means the group ID range is 0-0, that is disable ingress-mirror-groups.

The command to show the ranges of ingress-mirror-groups and egress-mirror-groups.

```
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges: default
  lag-select-groups=0-0
  ecmp-select-groups=0-0
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

The command to configure ingress-mirror-group and egress-mirror-group ID range:

ovs-vsctl set-group-ranges ingress-mirror-groups=*<min_value>-<max_value>*

or

ovs-vsctl set-group-ranges egress-mirror-groups=*<min_value>-<max_value>*

or

ovs-vsctl set-group-ranges ingress-mirror-groups=*<min_value1>-<max_value1>*,egress-mirror-groups=*<min_value2>-<max_value2>*

The group IDs may be divided into different areas: ingress-mirror-groups, egress-mirror-group and the original groups. The max range of group is 1-4294967039, and if configure different group the group range cannot conflict.

After configure the command, user need reboot switch.

Use command 'ovs-vsctl set-group-ranges' to back default group ranges.

```
admin@PicOS-OVS$ovs-vsctl set-group-ranges ingress-mirror-groups=1-10000,egress-mirror-groups=20000-30000

admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges:
  lag-select-groups=0-0
  ecmp-select-groups=0-0
  ingress-mirror-groups=1-10000
  egress-mirror-groups=20000-30000
```

Example 1

And ingress-mirror-group, first bucket modify packet's fields dl_vlan and dl_dst.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=100,type=all,bucket=set_field:100-\>vlan_vid,set_field:22:00:00:0(
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,dl_dst=22:11:11:11:11:11,actions=group:100
admin@PicOS-OVS$
```

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#1 normal permanent flow_id=6 (ingress mirror group) in_port=31,dl_dst=22:11:11:11:11:11, actions:set(eth_dst((dst=
Total 2 flows in HW.
admin@PicOS-OVS$
```

Example 2

And egress-mirror-group, first bucket modify packet's fields dl_src and dl_dst, second bucket is lag interface.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 -- set interface ae1 type=pica8_lag options:membe
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=20010,type=all,bucket=set_field:00:00:00:11:11:11-\>eth_src,set_f
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=31,actions=group:20010
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#2 normal permanent flow_id=7 (egress mirror group) in_port=31, actions:set(eth(src=00:00:00:11:11:11,dst=00:00:00
Total 2 flows in HW.
```

Close all Group-ranges

If user want close the group-ranges, please use command as below.

ovs-vsctl set-group-ranges

```
admin@PicOS-OVS$ovs-vsctl set-group-ranges
admin@PicOS-OVS$ovs-vsctl show-group-ranges
group_ranges:
  lag-select-groups=0-0
  ecmp-select-groups=0-0
  ingress-mirror-groups=0-0
  egress-mirror-groups=0-0
```

Configuring Controller or Manager

Connecting to a Controller

Use the OVSDB protocol to connect to a controller. The **ovs-vsctl** command requires an IP address and a port number on the OVS database server. In the example below, the switch connects to an OF controller with an IP address of 10.10.53.50, and port number of 6633.

```
root@PicOS-OVS# ovs-vsctl set-controller br0 tcp:10.10.53.50:6633
root@PicOS-OVS#
```

Verify connectivity with the controller:

```
admin@PicOS-OVS$ovs-vsctl show

101c4a95-2973-4aeb-9c0a-a04380950b4d
    Bridge "br0"
        Controller "tcp:10.10.53.50:6633"
            is_connected: true
        Port "te-1/1/50"
            tag: 1
            Interface "te-1/1/50"
                type: "pica8"
        Port "ge-1/1/48"
            tag: 1
            Interface "ge-1/1/48"
                type: "pica8"
        Port "br0"
            Interface "br0"
               type: internal
```

Check detailed controller status. A properly working controller configuration would appear as:

```
admin@PicOS-OVS$ovs-vsctl list controller

_uuid               : f35735f3-1d62-45ba-967e-59e324d1e150
auxiliary           : {}
connection_mode     : []
controller_burst_limit: []
controller_rate_limit: []
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : true
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : other
status              : {current_version="OpenFlow13", sec_since_connect="20", state=ACTIVE}
target              : "tcp:10.10.53.50:6633"
```

In the event of an error in the bridge configuration, such as a mismatch in the open flow version, the output would appear as:

```
admin@PicOS-OVS$ovs-vsctl list controller

_uuid               : f35735f3-1d62-45ba-967e-59e324d1e150
auxiliary           : {}
connection_mode     : []
controller_burst_limit: []
controller_rate_limit: []
```

```
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : true
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : other
status              : {last_error="Connection refused", sec_since_connect="7713",sec_since_disconnect="7721", state
target              : "tcp:10.10.53.50:6633"
```

Modify Openflow Protocol

PicOS supports openflow1.0, openflow1.2, openflow1.3, openflow1.4 default, if user wants special configuration openflow protocol number, the command is below.

ovs-vsctl set bridge br0 protocol=<OpenFlow protocol number>

```
admin@PicOS-OVS$ovs-vsctl set bridge br0 protocol=OpenFlow13
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl set bridge br0 protocol=OpenFlow10,OpenFlow13
```

Connection Mode between Bridge and Controller

From PicOS 2.4, the default connection between one bridge and all the controllers is in-band mode. User can configure to disable it, using the command as shown below.

ovs-vsctl set bridge br0 other_config=disable-in-band=<true|false>

Disable in-band mode. After disable in-band is done, all the controllers must use out-of-band mode connection to bridge, which means only the management port can be used to connect.

```
ovs-vsctl set bridge br0 other_config=disable-in-band=true
```

Enable in-band mode, all the controllers can use in-band connect to bridge.

```
ovs-vsctl set bridge br0 other_config=disable-in-band=false
```

If enabling in-band in bridge, user also can configure in-band or out-of-band in one single controller. That mean that this controller only uses out-of-band, Others still use in-band connect to bridge.

ovs-vsctl set controller [_uuid] connection_mode=out-of-band

```
admin@PicOS-OVS$ovs-vsctl list controller
_uuid               : 7f651b3b-4b0d-4d9b-b6e5-fe67499be1c4
auxiliary           : {}
connection_mode     : in-band
controller_burst_limit: []
controller_rate_limit: []
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : false
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : other
status              : {last_error="Network is unreachable", state=BACKOFF}
target              : "tcp:10.10.50.42:6653"
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl set controller 7f651b3b-4b0d-4d9b-b6e5-fe67499be1c4 connection_mode=out-of-band
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-vsctl list controller
_uuid               : 7f651b3b-4b0d-4d9b-b6e5-fe67499be1c4
auxiliary           : {}
connection_mode     : out-of-band
controller_burst_limit: []
controller_rate_limit: []
```

```
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : false
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : other
status              : {last_error="Network is unreachable", state=BACKOFF}
target              : "tcp:10.10.50.42:6653"
```

Auxiliary Connections

PicOS OVS supports Auxiliary connections to the controller. Auxiliary connections configuration is based on the OVS controller. When the user wants to use it, they must first configure auxiliary in the controller list.

ovs-vsctl set controller {uuid} auxiliary:{id}={udp | tcp}

Auxiliary configuration has two parameters:

- The first is Auxiliary ID, an integer that identifies auxiliary connections.

And the range is [1, 255].

- The second is a string that specifies the transport of auxiliary connection.

And now we only support “udp” and “tcp”.

Example:

Step 1: Assume there is a controller “tcp:10.10.51.16:6633” on Bridge br0 using this:

Firstly, get uuid of the controller using this:

```
ovs-vsctl set-controller br0 tcp:10.10.51.50:6633
```

Step 2: Get controller uuid:

```
ovs-vsctl list controller
admin@PicOS-OVS$ovs-vsctl list controller
_uuid               : 6eb5d036-87af-44ca-aa58-2b916ae126f4
auxiliary           : {}
connection_mode     : []
controller_burst_limit: []
controller_rate_limit: []
enable_async_messages: []
external_ids        : {}
inactivity_probe    : []
is_connected        : false
local_gateway       : []
local_ip            : []
local_netmask       : []
max_backoff         : []
other_config        : {}
role                : other
status              : {last_error="Connection refused", sec_since_disconnect="1", state=BACKOFF}
target              : "tcp:10.10.51.50:6633"
```

Step 3:

```
admin@PicOS-OVS$ovs-vsctl set controller 6eb5d036-87af-44ca-aa58-2b916ae126f4 auxiliary:1=udp
```

Configure Flow Table Flush once set or delete controller

ovs-vsctl set bridge br0 other_config:enable-flush=<true|false>

In PicOS OVS switch, the flow table will be cleared when user uses the **set-controller** command for the bridge. Starting with PicOS 2.6, user can define if the flow table is flushed or not by the **set-controller** and **del-controller** commands.

The flow table is flushed when **enable-flush=true**. The flow table is not flushed when **enable-flush=false**. The default value is **enable-flush=true**.

```
ovs-vsctl set bridge br0 other_config:enable-flush=true
ovs-vsctl set bridge br0 other_config:enable-flush=false
```

Display the configuration.

```
ovs-vsctl list Bridge
ovs-vsctl list bridge br0
```

Connecting to Manager

PicOS OVS supports connection to Manager.

Command to set manager as below,

```
admin@PicOS-OVS$ovs-vsctl set-manager ptcp:6640:10.10.51.49
or
admin@PicOS-OVS$ovs-vsctl set-manager tcp:10.10.51.49:6640
```

Before PicOS 2.6.5, manager is not supported by default. If user wants to connect manager, ovsdb-server must be restarted.

```
Kill following ovsdb-server:
ovsdb-server /ovs/ovs-vswitchd.conf.db /ovs/inventory.conf.db --pidfile --remote=ptcp:6640:10.10.51.138 --remote=pu

Then run ovsdb-server with --remote=db:Open_vSwitch,Manager,target:
ovsdb-server /ovs/ovs-vswitchd.conf.db /ovs/inventory.conf.db --pidfile --remote=ptcp:6640:10.10.51.138 --remote=pu
```

From PicOS 2.6.5, manager supported in ovsdb-server. Once user configures “ovs-vsctl set-manager tcp:10.10.51.49:6640”, user can connect manager by remote.

```
root@PicOS-OVS$ps aux | grep ovsdb-server
root      9598  0.1  0.1   7256  2816 pts/0    S    18:00   0:00 ovsdb-server /ovs/ovs-vswitchd.conf.db /tmp/invent
```

Before PicOS 2.7.1, when using command “ovs-vsctl set-manager tcp:10.10.51.49:6640” to connect manager, the manager’s “is_connected” is false, such like:

```
root@PicOS-OVS$ovs-vsctl list manager
_uuid               : 3cd2a235-6921-4580-a093-a3dd96431cc4
connection_mode     : []
external_ids        : {}
inactivity_probe    : []
is_connected        : false
max_backoff         : []
other_config        : {}
status              : {}
target              : "tcp:10.10.51.49:6640"
```

The behavior depends on the “remote” configuration.

If the “remote” is “db: Open_vSwitch,Manager, target”, the manager status will not be refreshed.

```
root@PicOS-OVS$ps aux | grep ovsdb-server
root      9598  0.1  0.1   7256  2816 pts/0    S    18:00   0:00 ovsdb-server /ovs/ovs-vswitchd.conf.db /tmp/invent
```

If the “remote” is “db: Open_vSwitch, Open_vSwitch, manager_options”, the manager status will be displayed right.

We can change the boot argument:

```
ovsdb-server /ovs/ovs-vswitchd.conf.db /tmp/inventory.conf.db /ovs/function.conf.db --pidfile --remote=ptcp:6640:12
```

Or we can use command to add this “remote”:

```
root@PicOS-OVS$ovs-appctl -t ovsdb-server ovsdb-server/add-remote db:Open_vSwitch,Open_vSwitch,manager_options
root@PicOS-OVS$ovs-vsctl list manager
_uuid               : 3cd2a235-6921-4580-a093-a3dd96431cc4
connection_mode     : []
external_ids        : {}
inactivity_probe    : []
is_connected        : true
max_backoff         : []
other_config        : {}
status              : {sec_since_connect="6", state=ACTIVE}
```

```
target              : "tcp:10.10.51.49:6640"
```

We can delete manager using command:

```
admin@PicOS-OVS$ovs-vsctl del-manager
```

From PicOS 2.7.1, user can list manager status correctly without re-configure ovsdb-server.

Creating SSL Connection to a Controller

- Creating SSL Connection to a RYU Controller
- Configure OVS Connection Using SSL with Self-signed Certificates

Creating SSL Connection to a RYU Controller

This section describes the procedure to create an SSL connection with the RYU controller.

PicOS Switch

The following steps need to be completed on the PicOS switch:

```
root@PicOS-OVS#apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  ca-certificates
The following NEW packages will be installed:
  openssl
0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.
Need to get 696 kB of archives.
After this operation, 1070 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  openssl
Authentication warning overridden.
Get:1 http://ftp.debian.org/debian/ stable/main openssl powerpc 1.0.1e-2 [696 kB]
Fetched 696 kB in 5s (131 kB/s)
Selecting previously unselected package openssl.
(Reading database ... 17049 files and directories currently installed.)
Unpacking openssl (from .../openssl_1.0.1e-2_powerpc.deb) ...
Processing triggers for man-db ...
Setting up openssl (1.0.1e-2) ...

root@PicOS-OVS#ovs-pki init
/ovs/bin/ovs-pki: /ovs/var/lib/openvswitch/pki already exists and --force not specified

root@PicOS-OVS#ovs-pki init --force
Creating controllerca...
Creating switchca...

root@PicOS-OVS#cd /ovs/var/lib/openvswitch/pki/controllerca

root@PicOS-OVS#ovs-pki req+sign ctl controller
ctl-req.pem     Mon Jan 13 03:26:05 UTC 2014
        fingerprint 1cbf63b21301f33d9b4aa30540bff492f15bced3

root@PicOS-OVS#ls
ca.cnf      careq.pem  crl        ctl-cert.pem     ctl-req.pem  index.txt.attr      index.txt.old  private  serial
cacert.pem  certs      crlnumber  ctl-privkey.pem  index.txt    index.txt.attr.old  newcerts       serial

root@PicOS-OVS#ls ctl-privkey.pem ctl-cert.pem
ctl-cert.pem  ctl-privkey.pem

root@PicOS-OVS#cd /ovs/var/lib/openvswitch/pki/switchca

root@PicOS-OVS#ovs-pki req+sign sc switch
sc-req.pem      Mon Jan 13 03:26:54 UTC 2014
        fingerprint 65ed449bee94b8e7b8ba7da6f6584afd2f9cc2fb

root@PicOS-OVS#ls sc-privkey.pem sc-cert.pem
sc-cert.pem  sc-privkey.pem

root@PicOS-OVS#
root@PicOS-OVS#scp /ovs/var/lib/openvswitch/pki/controllerca/ctl-cert.pem 10.10.50.41:/home/build
The authenticity of host '10.10.50.41 (10.10.50.41)' can't be established.
ECDSA key fingerprint is e6:04:3b:c8:24:36:c7:dd:c1:06:6a:69:e2:3b:82:2f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.50.41' (ECDSA) to the list of known hosts.
```

```
root@10.10.50.41's password:
ctl-cert.pem
                                                
```

Configure OVS Connection Using SSL with Self-signed Certificates

To make a SSL/TLS Openflow connection between onos and OVS switches using self-signed certificates, there are five main steps to follow:

1. *Generate SSL key/certificate for onos;*
2. *Test the SSL connection.*
3. *Copy the onos certificate to the appropriate OVS location so that OVS can accept the certificate from onos;*
4. *Generate SSL key/certificate for OVS;*
5. *Copy the OVS certificate to the appropriate onos location so that onos can accept the certificate from OVS;*

The following is an example of the detailed configuration steps.

Step 1. Generating SSL key/certificate for onos. On the host running onos, we generate the SSL key/certificate as the following:

a). Create a folder named “ssl”, in this folder we use "keytool" to generate a .jks keystone:

```
root@devel:/opt/onos# cd ssl
root@devel:/opt/onos/ssl# keytool -genkey -keyalg RSA -alias onos -keystore onos.jks -storepass 111111 -validity 3(
What is your first and last name?
  [Unknown]:  Ai Haoyu
What is the name of your organizational unit?
  [Unknown]:  FNLab-BUPT
What is the name of your organization?
  [Unknown]:  BUPT
What is the name of your City or Locality?
  [Unknown]:  Beijing
What is the name of your State or Province?
  [Unknown]:  Beijing
What is the two-letter country code for this unit?
  [Unknown]:  CN
Is CN=Ai Haoyu, OU=FNLab-BUPT, O=BUPT, L=Beijing, ST=Beijing, C=CN correct?
  [no]:  yes


Enter key password for <onos>
        (RETURN if same as keystore password):


Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard fo
root@devel:/opt/onos/ssl# ls
onos.jks
```

b). Covert the .jks keystore (which onos uses) to PEM file (which OVS uses) in a 2-step conversions: from .jks to .p12, then to .pem:

```
root@devel:/opt/onos/ssl# keytool -importkeystore -srckeystore onos.jks -destkeystore onos.p12 -srcstoretype jks -d
Importing keystore onos.jks to onos.p12...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias onos successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
root@devel:/opt/onos/ssl# ls
onos.jks  onos.p12
root@devel:/opt/onos/ssl# openssl pkcs12 -in onos.p12 -out onos.pem
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
root@devel:/opt/onos/ssl# ls
onos.jks  onos.p12  onos.pem
```

c). Use the certificate portion of the "onos.pem" file to create a new file, called "cacert.pem" - this is the file to be copied over to OVS - it is from "Bag Attributes" to "END CERTIFICATE":

```
root@devel:/opt/onos/ssl# cat onos.pem
<Private key here>
Bag Attributes
```

```
    friendlyName: onos
    localKeyID: 54 69 6D 65 20 31 35 33 39 33 32 37 38 34 32 31 39 39
subject=/C=CN/ST=Beijing/L=Beijing/O=BUPT/OU=FNLab-BUPT/CN=Ai Haoyu
issuer=/C=CN/ST=Beijing/L=Beijing/O=BUPT/OU=FNLab-BUPT/CN=Ai Haoyu
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIEOtHFEDANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJD
TjEQMA4GA1UECBMHQmVpamluZzEQMA4GA1UEBxMHQmVpamluZzENMAsGA1UEChME
......
-----END CERTIFICATE-----



root@devel:/opt/onos/ssl# sudo vi ./cacert.pem
Bag Attributes
    friendlyName: onos
    localKeyID: 54 69 6D 65 20 31 35 33 39 33 32 37 38 34 32 31 39 39
subject=/C=CN/ST=Beijing/L=Beijing/O=BUPT/OU=FNLab-BUPT/CN=Ai Haoyu
issuer=/C=CN/ST=Beijing/L=Beijing/O=BUPT/OU=FNLab-BUPT/CN=Ai Haoyu
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIEOtHFEDANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJD
TjEQMA4GA1UECBMHQmVpamluZzEQMA4GA1UEBxMHQmVpamluZzENMAsGA1UEChME
.......
-----END CERTIFICATE-----
```

Note:

The intermediate key/cert, "onos.p12", and onos.pem, are no longer used and should be discarded.

Step 2. Copy the onos certificate to the appropriate OVS location so that OVS can accept the certificate from onos:

a). In the case of PicaOS, firstly we need to install openssl module, then create controllerca directory and switchca directory, and generate key and certificate for the OVS switch in switchca directory:

```
admin@PICOS-OVS:~$ sudo apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
admin@PICOS-OVS:~$ sudo su
root@PICOS-OVS:/home/admin# ovs-pki init --force
Creating controllerca...
Creating switchca...
root@PICOS-OVS:~$ cd /ovs/var/lib/openvswitch/pki/switchca
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/switchca# ovs-pki req+sign sc switch
sc-req.pem      Mon Oct 15 16:01:11 UTC 2018
        fingerprint 0d336057404dab9bc7dc158b7f4a7007ced6efd4
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/switchca# ls -lat
total 76
drwxr-xr-x 6 root root 4096 Oct 15 16:01 .
.....
-rw-r--r-- 1 root root 4002 Oct 15 16:01 sc-cert.pem
-rw-r--r-- 1 root root 3565 Oct 15 16:01 sc-req.pem
-rw------- 1 root root 1675 Oct 15 16:01 sc-privkey.pem
-rw-r--r-- 1 root root 4028 Oct 15 15:56 cacert.pem
....
drwxr-xr-x 4 root root 4096 Oct 15 15:56 ..
```

a). Copy cacert.pem from your ONOS working directory(/opt/ssl) to this directory your OVS machine: "/ovs/var/lib/openvswitch/pki/controllerca/cacert.pem", you can replace or backup the original cacert.pem file.

```
root@PICOS-OVS:/etc# mkdir ovsbackup
root@PICOS-OVS:/etc# cd ovsbackup/
root@PICOS-OVS:/etc/ovsbackup# cd /ovs/var/lib/openvswitch/pki/controllerca
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/controllerca# ls
ca.cnf  cacert.pem  careq.pem  certs  crl  crlnumber  index.txt  index.txt.attr  index.txt.old  newcerts  private
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/controllerca# mv cacert.pem /etc/ovsbackup/
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/controllerca# ls
ca.cnf  careq.pem  certs  crl  crlnumber  index.txt  index.txt.attr  index.txt.old  newcerts  private  serial  ser
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/controllerca# scp pica8@10.10.50.243:/opt/ssl/cacert.pem .
The authenticity of host '10.10.50.243 (10.10.50.243)' can't be established.
```

```
ECDSA key fingerprint is a3:a4:a2:ab:a9:bd:81:02:16:7a:9b:8d:f9:07:e3:90.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.50.243' (ECDSA) to the list of known hosts.
pica8@10.10.50.243's password:
cacert.pem
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/controllerca# ls
ca.cnf  cacert.pem  careq.pem  certs  crl  crlnumber  index.txt  index.txt.attr  index.txt.old  newcerts  private
```

c). Make OVS to use the new keys:

```
root@PICOS-OVS:/ovs/var/lib/openvswitch/pki/switchca# ovs-vsctl set-ssl /ovs/var/lib/openvswitch/pki/switchca/sc-pr
```

Step 3. Copy the OVS certificate to the appropriate onos location so that onos can accept the certificate from OVS:

a). Copy "sc-cert.pem" (the OVS public key just generated in 2.1) to the ONOS host, and import it to onos.jks store with trust:

```
root@pica8:/opt/ssl# scp admin@10.10.51.140:/ovs/var/lib/openvswitch/pki/switchca/sc-cert.pem .
The authenticity of host '10.10.51.140 (10.10.51.140)' can't be established.
ECDSA key fingerprint is SHA256:3hI1TnyjNj2k7QgjCRS5xR/2wh5yxKijgwMHIuCsm0s.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.51.140' (ECDSA) to the list of known hosts.
admin@10.10.51.140's password:
sc-cert.pem
root@pica8:/opt/ssl# ls
cacert.pem  onos.jks  onos.p12  onos.pem  sc-cert.pem
root@pica8:/opt/ssl# keytool -importcert -file sc-cert.pem -keystore onos.jks
Enter keystore password:
Owner: CN=sc id:2018 Oct 15 16:01:09, OU=Open vSwitch certifier, O=Open vSwitch, ST=CA, C=US
Issuer: CN=OVS switchca CA Certificate (2018 Oct 15 15:56:46), OU=switchca, O=Open vSwitch, ST=CA, C=US
Serial number: 2
Valid from: Tue Oct 16 00:01:11 CST 2018 until: Fri Oct 13 00:01:11 CST 2028
Certificate fingerprints:
         MD5:  AA:53:F9:43:D4:77:07:38:87:25:DC:3D:8A:0A:19:A6
         SHA1: 45:19:64:D8:E1:A7:2A:18:CC:15:25:10:9A:C8:AE:BC:FD:53:AB:CC
         SHA256: 75:BE:13:3D:DB:8E:DC:39:D1:73:01:A8:A3:04:00:9B:D1:7B:98:84:49:85:2A:B9:5C:E9:1D:B6:F6:45:C5:E0
Signature algorithm name: MD5withRSA (weak)
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1

Warning:
The input uses the MD5withRSA signature algorithm which is considered a security risk.

Trust this certificate? [no]:  yes
Certificate was added to keystore


Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard fo
root@pica8:/opt/ssl# keytool -list -keystore onos.jks
Enter keystore password:
Keystore type: jks
Keystore provider: SUN


Your keystore contains 2 entries

onos, Oct 15, 2018, PrivateKeyEntry,
Certificate fingerprint (SHA1): F9:D6:36:06:B8:5A:AE:0C:50:CE:B8:E3:DF:16:0F:9B:5C:8B:2E:7C
mykey, Oct 15, 2018, trustedCertEntry,
Certificate fingerprint (SHA1): 45:19:64:D8:E1:A7:2A:18:CC:15:25:10:9A:C8:AE:BC:FD:53:AB:CC
```

b). In the ONOS host, make sure these applications are activated:

```
onos> apps -s
......
*  21 org.onosproject.hostprovider         1.13.3   Host Location Provider
*  22 org.onosproject.lldpprovider         1.13.3   LLDP Link Provider
*  23 org.onosproject.optical-model        1.13.3   Optical Network Model
```

```
*  24 org.onosproject.openflow-base        1.13.3   OpenFlow Base Provider
*  25 org.onosproject.openflow             1.13.3   OpenFlow Provider Suite
......
*  37 org.onosproject.drivers              1.13.3   Default Drivers
......
```

c). Enable ONOS to use OFTLS by configuring "$ONOS_HOME/bin/onos-service":

```
root@pica8:/opt/onos/bin# vi onos-service
#!/bin/bash
# -----------------------------------------------------------------------------
# Starts ONOS Apache Karaf container
# -----------------------------------------------------------------------------


# uncomment the following line for performance testing
# export JAVA_OPTS="${JAVA_OPTS:--Xms16G -Xmx16G -XX:+UseConcMarkSweepGC -XX:+CMSIncrementalMode -XX:+PrintGCDetail


# uncomment the following line for Netty TLS encryption
# Do modify the keystore location/password and truststore location/password accordingly
#export JAVA_OPTS="${JAVA_OPTS:--DenableNettyTLS=true -Djavax.net.ssl.keyStore=/home/ubuntu/onos.jks -Djavax.net.ss


export JAVA_OPTS="${JAVA_OPTS:--DenableOFTLS=true -Djavax.net.ssl.keyStore=/opt/ssl/onos.jks -Djavax.net.ssl.keySto


export JAVA_OPTS="${JAVA_OPTS:--Dds.lock.timeout.milliseconds=10000}"

set -e  # exit on error
set -u  # exit on undefined variable
................
"onos-service" 57L, 2308C written
```

c). Restart the ONOS controller.

Step 4. Testing the SSL connection:

a). On the OVS machine, we create a new bridge named br0, and set it connect to the controller by ssl:

```
admin@PICOS-OVS:/$ ovs-vsctl add-br br0 - set bridge br0 datapath_type=pica8
admin@PICOS-OVS:/$ ovs-vsctl show
5187ffd7-d781-48dc-82a6-37692344a877
    Bridge "br0"
        Port "br0"
            Interface "br0"
                type: internal
admin@PICOS-OVS:/$ ovs-vsctl set-controller br0 ssl:10.10.50.243:6653
```

b). Check the OVS machine log, You should see the following log messages:

```
admin@PICOS-OVS:~$ tail -f /tmp/log/messages
Oct 15 2018 17:39:54 Xorplus daemon.notice : 17:39:54.742|ovs|00879|rconn|INFO|br0<->ssl:10.10.50.243:6653: connect
Oct 15 2018 17:40:06 Xorplus daemon.notice : 17:40:06.390|ovs|00880|connmgr|INFO|br0<->ssl:10.10.50.243:6653: 3 flo
```

c). Check the device on ONOS host, you can see the OVS machine in the list:

```
onos> devices
id=of:1c480030ab283b4f, available=true, local-status=connected 25m15s ago, role=MASTER, type=SWITCH, mfr=Pica8, Inc
```

We can see the SSL connection is successful.

Configuring Counter

Clear counter

Clear port counter

Command: ovs-appctl bridge/clear-counts br0

User can use above command to clear the port counter.

Example:

```
Check port counter:
ovs-ofctl dump-ports br0

Clear the port counter:
ovs-appctl bridge/clear-counts br0
```

Clear flow counter

Command: ovs-ofctl mod-flows br0 reset_counts,<match>,<actions>

User can use the command to clear flow counter.

Example:

```
ovs-ofctl add-flow br0 in_port=3,actions=4
ovs-ofctl mod-flows br0 reset_counts,in_port=3,actions=4
```

Drop counter

Pica8 has added support for drop counter from PicOS version 2.7.2. This feature is useful in cases where we need to count the dropped packets. For this counter, we use rdbgc4 register to count the dropped packets.

The command is:

```
ovs-vsctl set-rdbgc4 [TYPE]
```

TYPE value: **rfldr; ripd4; ripd6; riphe6; vlandr**

Default value: **rfldr**

Use the command below to display rdbgc4 setting.

```
 ovs-vsctl show-rdbgc4
```

The command below is used get drop statistics on a given port.

```
ovs-ofctl dump-drop br0 [PORT]
```

1. rdbgc4 drop counter values:

1)ovs-vsctl set-rdbgc4 rfldr

Setting the rdbgc4 value to rfldr will count the packets which are dropped by a drop action (actions=drop) flow in TCAM. Packets matching this flow are dropped and drop statistics are recorded in the drop counter.

Example:

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/9 vlan_mode=trunk tag=1  -- set Interface te-1/1/9 type=pica8
ovs-vsctl add-port br0 te-1/1/10 vlan_mode=trunk tag=1  -- set Interface te-1/1/10 type=pica8
```

Packets will match default drop flow without configuring flows.

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
      Statistics type in rdbgc4: rfldr
        Discarded  Packets.................10000
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................10000
```

2) ovs-vsctl set-rdbgc4 vlandr

Count the packets whose tag doesn't match the ingress port's VLAN ID.

Example:

```
ovs-vsctl add-port br0 te-1/1/9 vlan_mode=access tag=10  -- set Interface te-1/1/9 type=pica8
ovs-vsctl add-port br0 te-1/1/10 vlan_mode=trunk tag=1  -- set Interface te-1/1/10 type=pica8
```

add flow:

```
ovs-ofctl add-flow br0 in_port=9,actions=10
```

Send packets with vlan=199 to port 10 and check drop counter.

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
      Statistics type in rdbgc4: vlandr
        Discarded  Packets.................10000
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................0
```

If modify flow actions=drop,after above steps, ingress drop caused by flow-match will have discarded packets statistics 10000.

3) ovs-vsctl set-rdbgc4 ripd4

Count the ipv4 packets which send to route table with VLAN **CFI=set or TTL=0**.

Example:

```
ovs-vsctl set-l2-mode true
ovs-vsctl set-l3-mode true
ovs-ofctl add-flow br0 table=251, dl_vlan=199,dl_dst=22:22:22:22:22:22,actions=normal
ovs-ofctl add-flow br0 table=252, ip,nw_dst=2.2.2.2,actions=set_field: 00:00:00:00:22:22-\>dl_dst,set_field:1999-\>
```

Send packets with dl_dst=22:22:22:22:22:22, dl_dst=22:11:11:11:11:11,dl_vlan=199,**CFI=SET**, nw_dst=2.2.2.2, nw_src=1.1.1.1 to port 10.

Check drop counter:

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
      Statistics type in rdbgc4: ripd4
        Discarded  Packets.................10000
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................0
```

4) ovs-vsctl set-rdbgc4 ripd6

Count the ipv6 packets which send to route table with **VLAN CFI=set or Hop=0**.

Example:

```
ovs-vsctl set-l2-mode true
ovs-vsctl set-l3-mode true
ovs-ofctl add-flow br0 table=251,dl_vlan=199,dl_dst=22:22:22:22:22:22,actions=normal
ovs-ofctl add-flow br0 table=252,ipv6,ipv6_dst=2001::1,actions=set_field: 00:00:00:00:22:22-\>dl_dst,set_field:199
```

Send packets with dl_dst=22:22:22:22:22:22, dl_dst=22:11:11:11:11:11,dl_vlan=199,**CFI=RESET, hop=0,** ipv6_dst=2001::1,ipv6_src=2002::1 to port 10:

Check drop counter:

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
       Statistics type in rdbgc4: ripd6
        Discarded  Packets.................10000
      Statistics type : ingress drop caused by congestion (bytes)
```

```
        Discarded  Octets.................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets.................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................0
```

5) ovs-vsctl set-rdbgc4 riphe6

Count the ipv6 packets which send to route table with **ipv6_dst=::**

Example:

```
ovs-vsctl set-l2-mode true
ovs-vsctl set-l3-mode true
ovs-ofctl add-flow br0 table=251,dl_vlan=199,dl_dst=22:22:22:22:22:22,actions=normal
ovs-ofctl add-flow br0 table=252,ipv6,ipv6_dst=2001::1,actions=set_field:00:00:00:00:22:22-\>dl_dst,set_field:1999
```

Send packets with dl_dst=22:22:22:22:22:22,dl_dst=22:11:11:11:11:11,dl_vlan=199, ipv6_dst=0::0,ipv6_src=2002::1

Check drop counter:

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
       Statistics type in rdbgc4: riphe6
        Discarded  Packets.................10000
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets.................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets.................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................0
```

2.Congest drop counter:

Count packets which dropped because of congestion.

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
      Statistics type in rdbgc4: rfldr
        Discarded  Packets.................0
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets.................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets.................22567715016
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................331876187
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................0
```

3.ingress drop counter:

the packets which dropped by the actions=drop flow in tcam.

Example：

```
ovs-ofctl add-flow br0 in_port=9,ip,dl_vlan=199,nw_dst=192.168.100.100,actions=drop
```

Send packets to match this flow and check drop counter:

```
admin@PicOS-OVS$ovs-ofctl dump-drop br0 9
PXST_DROP_STATS reply (OF1.4) (xid=0x2): 1 interfaces
  te-1/1/9(port 9):
    Statistics type in rdbgc4: vlandr
        Discarded  Packets.................0
      Statistics type : ingress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : ingress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : egress drop caused by congestion (bytes)
        Discarded  Octets..................0
      Statistics type : egress drop caused by congestion (packets)
        Discarded  Packets.................0
      Statistics type : ingress drop caused by flow-match (packets)
        Discarded  Packets.................10000
```

1.Drop counter only works in ingress,but when congest statistics is in egress.

2.User can use following command to clear statistics：

ovs-appctl bridge/clear-counts br0

Counter Interval

The default flow counter interval is 500ms and port counter interval is 1000~1200ms. User can shorten the flow interval time and from PicOS-2.11 can shorten the port interval, but this will cause switch cpu busy.

Flow counter interval

By default, the flow counter interval is about 500ms. User can use following cammand to change it.

ovs-vsctl set open_vswitch . other_config:max-idle=<ms>

<ms>: 1~500 ms, the max interval is 500ms.

Example:

```
admin@PICOS-OVS$ovs-vsctl set open_vswitch . other_config:max-idle=100
```

Port Counter Interval

By default, the flow counter interval is about 1000~1200ms. User can use following cammand to change it.

ovs-vsctl set-counter-interval <ms>

<ms>: 10~1000 ms, the max interval is 1000ms.

Example:

```
admin@PICOS-OVS$ovs-vsctl set-counter-interval 100
```

Port Counter Interval

By default, the flow counter interval is about 1000~1200ms. User can use following cammand to change it.

ovs-vsctl set-counter-interval <ms>

<ms>: 10~1000 ms, the max interval is 1000ms.

Example:

```
admin@PICOS-OVS$ovs-vsctl set-counter-interval 100
```

Switching Open vSwitch version

Pica8 also support ovs 2.6 from version 2.11.0, and following command is used for switching between ovs 2.3 and ovs 2.6. System enter ovs 2.3 default.

Switch ovs from 2.3 to 2.6:

```
admin@PICOS-OVS$switch-to-ovs-2.6
```

And switch ovs from 2.6 to 2.3:

```
admin@PICOS-OVS$switch-to-ovs-2.3
```

If you swith ovs from 2.3 to 2.6,you had better to exit firstly and then enter system again. And some commands and functions are diferent from ovs 2.3.

Following table is the difference between ovs 2.3 and ovs 2.6.

Points	Ovs 2.3	Ovs 2.6
Pid in hardware table	userspace(pid=0,slow_path(lldp))	userspace(slow_path(lldp))
Ovs-appctl pica/dump-flows	Normal permanent;not distinguish table show	table_miss; distinguish table show
Arp/icmpv6 proxy	Flow priority in hardware table is 2	Flow priority in hardware table is the same with softeare table
Eviction in ovs-ofctl dump-tables-desc br0	0: config: EVICTION, eviction_flag: OTHER LIFETIME	show with vacancy together
Vacancy in ovs-ofctl dump-tables-desc br0	0: config: VACANCY_EVENTS, vacancy: 0%, vacancy_down: 20%, vacancy_up: 50%	show with eviction together
Enable-packet-driven	support	not support
TTP	support	not support
L3 table using lag/ecmp select group	ttl-1	ttl not change,keep primary value if not modified
Ovs-vsctl **Keep-l3-egress-fields**	support	delete
Ovs-appctl pica/dump-ecmp-flows	/	new command
Down one port when do ecmp select hash	output number stay the same	output number dynamic changed according ports' up/down
Multitable	dl_src changed to system mac if actions have no dl_src modification	keep primary value if actions have no dl_src modification
Ovs-vsctl set-select-group-hash-fields	Not clear flows in table 0	Clear flows in table 0
Ovs-ofctl queue-get-config br0 index	Queue get configure based port index	Queue get configure based port index or bridge
Ovs-appctl loopback/enable true	support	delete
Flows with same match filed except priority	Flow with high priority to hardware table	All flows installed to hardware table directly
Set match mode	ovs-appctl pica/dump-flows have echo	ovs-appctl pica/dump-flows have no echo

Configuring rate limit

From 2.11.16, Pica8 support configuring rate limit for port. Interface-based rate limiting controls the total rate of all packets passing through an interface to ensure that the bandwidth usage is within the allowed range. For the same interface, you can configure interface-based rate limiting in both ingress and egress directions or in only one direction.

1, Configuring ingress interface-based rate limt

If you do not limit the traffic sent by users, the continuous burst of data of a large number of users will make the network more crowded. By configuring the ingress interface-based rate limiting on the interface, you can limit the traffic entering the interface to a reasonable range.

Command:

```
ovs-vsctl set interface <ingress-port> ingress_policing_rate=<value1>
ovs-vsctl set interface <ingress-port> ingress_policing_burst=<value2>
```

Note:

(1) The unit is kbps.

(2) These commands can only apply on physical ports.

(3) When there is none burst configure,ingress_policing_burst is equal to ingress_policing_rate.

Configuration example:

Set the rate limit 300000 on ingress port for the ingress traffic.

1)create bridge and add ports to bridge.

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1
```

2)add flow.

```
ovs-ofctl add-flow br0 in_port=1,actions=2
```

3)configure ingress rate limit on te-1/1/1.

```
ovs-vsctl set interface te-1/1/1 ingress_rate_limit=300000
```

And after above configuration, you can limit the traffic entering to te-1/1/1 as 300M.

2, Configuring egress interface-based rate limt

To control the rate of all outgoing traffic on an interface, configure egress interface-based rate limiting. When the transmit rate of packets exceeds the configured rate limit, the excess packets will be discarded.

Command:

```
ovs-vsctl set interface <egress-port> egress_policing_rate=<value1>
ovs-vsctl set interface <egress-port> egress_policing_burst=<value2>
```

Note:

(1) The unit is kbps.

(2) These commands can only apply on physical ports.

(3) When there is none burst configure,egress_policing_burst is equal to egress_policing_rate.

Configuration example:

Set the rate limit 300000 on egress port for the egress traffic.

1)create bridge and add ports to bridge.

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1
ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1
```

2)add flow.

```
ovs-ofctl add-flow br0 in_port=1,actions=2
```

3)configure egress rate limit on te-1/1/1.

```
ovs-vsctl set interface te-1/1/2 egress_rate_limit=300000
```

And after above configuration,when the transmit rate of packets exceeds 300M, the excess packets will be discarded

Configuring IPv4/IPv6 address for management port

Introduction

Now support configure ipv4 and ipv6 address for eth0 from 3.2.1 for NPB.And support this feature from 3.4.0.When change ovs mode from l2/l3,there are some options for users to select.Such as the following example:

sudo picos_boot->chose '2',then you can chose how to configure the IP(IPv4) of management interface,DHCP or static IP.And then you can choose how to configure the ip(ipv6) of management interface,DHCP/Static IP/SLAAC/Disable IPv6.

Description

configure ipv4 or ipv6 address example.

```
admin@Xorplus:~$ sudo picos_boot
Configure the default system start-up options:
(Select key 3 if no change)
[1]  PICOS L2/L3   * default
[2]  PICOS Open vSwitch/OpenFlow
[3]  No start-up changeEnter your choice (1,2,3):2
PICOS Open vSwitch/OpenFlow is selected.
Configure the IP(IPv4) of management interface:
[1] DHCP    * default
[2] Static IP
Enter your choice(1,2):1
Configure the IP(IPv6) of management interface:
[1] DHCP
[2] Static IP
[3] SLAAC
[4] Disable IPv6    * default
Enter your choice(1,2,3,4):4
Start OVS web user interface?(y|n)[n]:y
Start OVS network snmp?(y|n)[n]:y
Please restart the PICOS service
```

Configuring the Duplex Mode of Optical Port

Thenew command configures the duplex mode of optical port as auto negotiation mode.

Command Syntax

ovs-vsctl set interface <*interface-name*> **options:duplex=auto**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>**>**	Specifies the optical port name.

Usage Guidelines

Pay attention to the following notes:

- Currently, duplex mode for optical port is only available for the 10 optical port when its port rate set to 1G.
- Duplex mode for optical port currently only supports to configure as auto, i.e. auto negotiation mode.
- It is required that the duplex mode of the peer 1G optical port is also set to auto negotiation mode, otherwise the port cannot link up.

Use command **delete interface gigabit-ethernet** <*interface-name*> **duplex** to go back to the default duplex mode to full.

Example

- Set the duplex mode of optical port te-1/1/1 as auto negotiation mode.

```
admin@PICOS-OVS:~$ovs-vsctl set interface te-1/1/1 options:link_speed=1G
admin@PICOS-OVS:~$ovs-vsctl set interface te-1/1/1 options:duplex=auto
```

Configuring Port Speed on AS9716-32D and N9550-32D

Step 1 Configure port lane mode before set port speed. To make this configuration effective, users have to restart PICOS service after the configuration.

ovs-vsctl set-port-lane-mode {**all** | <*port_number*>} <**0**|**1**>

- **all** | <*port_number*>: specifies the port number. **all** indicates to configure for all ports. <*port_number*> indicates the port number on the front panel, for example, number 10 represents port xe-1/1/10.
- **0**|**1**: specifies the port lane mode. **0** indicates 8 lanes, supporting port speed 400Gb/s. **1** indicates 4 lanes, supporting port speed 100Gb/s.

By default, the port lane mode is **0**.

The following command configures the lane mode of port xe-1/1/10 to 1 to support speed 100Gb/s.

```
admin@PICOS-OVS:~$ ovs-vsctl set-port-lane-mode 10 1

  Port 10 has been set lane_mode=1!
  Please reboot for the change to take effect!
```

Step 2 Restart PICOS service after the configuration to make the configuration effective.

```
admin@PICOS-OVS:~$ sudo systemctl restart picos
```

Step 3 Show port information. From the show result, we can see that lane mode of port xe-1/1/10 has been set to 1.

```
admin@PICOS-OVS:~$ ovs-vsctl show-valid-port
Front Sub BreakOut IfIndex Quad-Group Interface-Name Lane-Mode Configurable-Speed
----- --- -------- ------- ---------- -------------- --------- ------------------
 1     1   False    129     N/A        xe-1/1/1       0         400G,100G
 2     1   False    130     N/A        xe-1/1/2       0         400G,100G
 3     1   False    131     N/A        xe-1/1/3       0         400G,100G
 4     1   False    132     N/A        xe-1/1/4       0         400G,100G
 5     1   False    133     N/A        xe-1/1/5       0         400G,100G
 6     1   False    134     N/A        xe-1/1/6       0         400G,100G
 7     1   False    135     N/A        xe-1/1/7       0         400G,100G
 8     1   False    136     N/A        xe-1/1/8       0         400G,100G
 9     1   False    137     N/A        xe-1/1/9       0         400G,100G
 10    1   False    138     N/A        xe-1/1/10      1         400G,100G
 11    1   False    139     N/A        xe-1/1/11      0         400G,100G
 12    1   False    140     N/A        xe-1/1/12      0         400G,100G
.......
```

Step 4 Configure the port speed.

```
admin@PICOS-OVS:~$ ovs-vsctl add-port br0 xe-1/1/10
admin@PICOS-OVS:~$ ovs-vsctl set interface xe-1/1/10 options:link_speed=100G
```

Step 5 Show bridge information. From the result, we can see that the link speed of port xe-1/1/10 has been set to 100G.

```
admin@PICOS-OVS:~$ ovs-vsctl show
ab0f08dc-9262-43f1-9894-d82c62827a06
    Bridge "br0"
        Port "br0"
            Interface "br0"
                type: internal
```

```
        Port "xe-1/1/25"
            tag: 3
            Interface "xe-1/1/25"
                type: "pica8"
        Port "xe-1/1/10"
            Interface "xe-1/1/10"
                options: {link_speed="100G"}
        Port "xe-1/1/26"
            tag: 4
            Interface "xe-1/1/26"
                type: "pica8"
```

Examples and Topologies

This chapter provides configuration examples for 802.1Q.

- GRE Tunnel
- Multiple Virtual Bridges
- SSL Connection to Controller
- ECMP
- 802.1Q VLAN
- MPLS Network

802.1Q VLAN

In the following topology, user needs to configure 2 VLANs in switches A and B.

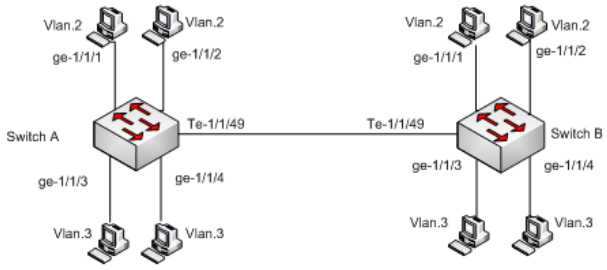


Figure 4-1. 802.1Q network configuration

Configure Switch-A

In Switch-A, user needs to configure ge-1/1/1~ge-1/1/4 as access port while configuring te-1/1/49 as trunk port because the 10Gbit link will trunk the traffic of VLAN-2 and VLAN-3.

```
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/1 vlan_mode=access tag=2 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/2 vlan_mode=access tag=2 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/3 vlan_mode=access tag=3 -- set Interface te-1/1/3 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/4 vlan_mode=access tag=3 -- set Interface te-1/1/4 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/49 vlan_mode=trunk trunk=2,3 -- set Interface te-1/1/49 type=pica8
root@PicOS-OVS#
```

Configure Switch-B

In Switch-B, user needs to configure ge-1/1/1~ge-1/1/4 as access port while te-1/1/49 as trunk port because the 10Gbit link will trunk the traffic of VLAN-2 and VLAN-3.

```
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/1 vlan_mode=access tag=2 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/2 vlan_mode=access tag=2 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/3 vlan_mode=access tag=3 -- set Interface te-1/1/3 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/4 vlan_mode=access tag=3 -- set Interface te-1/1/4 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/49 vlan_mode=trunk trunk=2,3 -- set Interface te-1/1/49 type=pica8
root@PicOS-OVS#
```

ECMP

```
root@PicOS-OVS#ovs-vsctl  del-br br0
root@PicOS-OVS#ovs-vsctl  add-br br0 -- set bridge br0 datapath_type=pica8
root@PicOS-OVS#ovs-vsctl  add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 trunks=1000,2000,3000,4094 -- set Interface g
root@PicOS-OVS#ovs-vsctl  add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 trunks=1000,2000,3000,4094 -- set Interface g
root@PicOS-OVS#ovs-vsctl  add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 trunks=1000,2000,3000,4094 -- set Interface g
root@PicOS-OVS#ovs-vsctl  add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 trunks=1000,2000,3000,4094 -- set Interface g
root@PicOS-OVS#ovs-ofctl del-flows br0
root@PicOS-OVS#ovs-ofctl add-group br0 group_id=1,type=select,bucket=output:2,bucket=output:3,bucket=output:4
root@PicOS-OVS#ovs-vsctl set-l3-mode true
root@PicOS-OVS#ovs-ofctl add-flow br0 table=251,dl_dst=22:22:22:22:22:22,dl_vlan=10,actions=normal
root@PicOS-OVS#ovs-ofctl add-flow br0 dl_type=0x0800,nw_dst=192.168.2.0/24,actions=group:1
```

Send packets (nw_dst incr number is 200) to Port 1,

Packets whose nw_dst= 192.168.2.0/255.255.255.3 will be forwarded to Port 2.

Packets whose nw_dst= 192.168.2.1/255.255.255.3 will be forward to Port 3.

Packets whose nw_dst= 192.168.2.2/255.255.255.3 will be forward to Port 4.

Packets whose nw_dst= 192.168.2.3/255.255.255.3 will be forward to Port 2.

GRE Tunnel

In the following topology, the GRE tunnel between Switches A and B needs to be configured. The IP address of the GRE tunnel is 10.10.61.10/24 and 10.10.60.10/24.

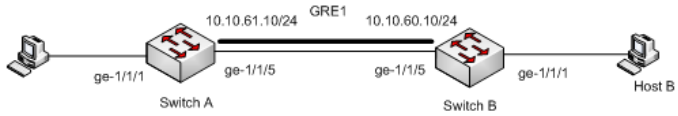


Figure 4-2. GRE tunnel configuration

Configure Switch-A

In Switch-A, user needs to configure a GRE tunnel and two flows as follows:

```
root@PicOS-OVS# ovs-vsctl  add-br br0 -- set bridge br0 datapath_type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set Interface ge-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 ge-1/1/5 vlan_mode=trunk tag=1 -- set Interface ge-1/1/5 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.60.10 opt
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:3073
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=5,actions=mod_dl_src:00:11:11:11:11:11,mod_dl_dst:00:33:33:33:33:33
```

Configure Switch-B

In Switch-A, user also needs to configure a GRE tunnel and two flows as follows:

```
root@PicOS-OVS# ovs-vsctl  add-br br0 -- set bridge br0 datapath_type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set Interface ge-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 ge-1/1/5 vlan_mode=trunk tag=1 -- set Interface ge-1/1/5 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl  add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.61.10 opt
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,actions=output:3073
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=5,actions=mod_dl_src:00:22:22:22:22:22,mod_dl_dst:00:66:66:66:66:66
```

MPLS Network

The Pica8 PICOS network operating system can run in two different modes:

- OVS (Open vSwitch) mode, in which PICOS is optimized for OpenFlow applications
- L2/L3 (Layer 2/Layer 3) mode, where PICOS can run traditional switching and routing protocols, as well as OpenFlow applications

In OVS mode, L2/L3 daemons are turned off and the switch is dedicated to OpenFlow and OVS. In this mode, PICOS open white box switches can support various configurations, including 802.1Q VLANs, Multiple Virtual Bridges, SSL Connection to Controller and Multiprotocol Label Switching (MPLS).

MPLS is a technique for routing traffic across a network using short path labels rather than long network addresses. It is intended to more efficiently and quickly route traffic across a network by avoiding routing table lookups and potentially circuitous routes to a destination.

This document describes how to configure PICOS for an MPLS network.

Traffic (Red) from host-A to host-B is forward by the MPLS network with Label 10. The traffic (Blue) from host-C to host-D is forwarded by the MPLS network with Label 20. All the flows will only push one MPLS header.

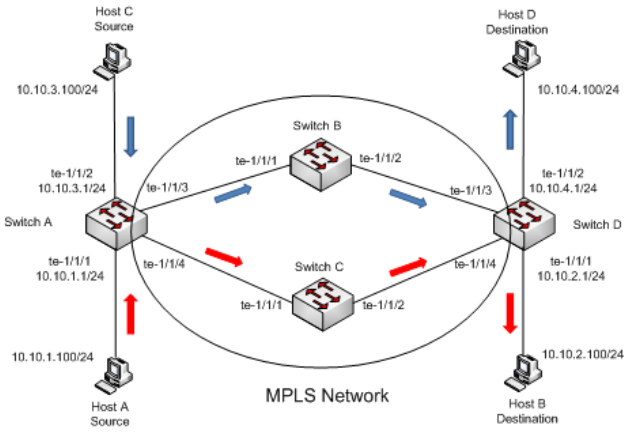


Figure 4-2. MPLS network configuration

Configure Switch-A

In Switch-A, user needs to configure two flows, which will push the MPLS Label 10 and 20 for traffic RED and BLUE, respectively.

```
root@PicOS-OVS# ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
device br0 entered promiscuous mode
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/1 vlan_mode=access tag=1 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/2 vlan_mode=access tag=1 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/3 vlan_mode=access tag=1 -- set Interface te-1/1/3 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/4 vlan_mode=access tag=1 -- set Interface te-1/1/4 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=10.10.1.100,nw_dst=10.10.2.100,dl_vlan=1,act
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=2,dl_type=0x0800,nw_src=10.10.3.100,nw_dst=10.10.4.100,dl_vlan=1,act
root@PicOS-OVS#
```

The received packet format in port te-1/1/1 and te-1/1/2 is shown as follows (ingress):

Ethernet	IP Header

The transmitted packet format to port te-1/1/3 and te-1/1/4 is shown as follows (egress):

Ethernet	MPLS label 10	IP Header

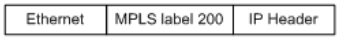
Ethernet	MPLS label 20	IP Header

Configure Switch-B

In Switch-B, user needs to configure one flow, which will SWAP the MPLS Label 20 to 200 for traffic BLUE.

```
root@PicOS-OVS# ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
device br0 entered promiscuous mode
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/1 vlan_mode=access tag=1 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/2 vlan_mode=access tag=1 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x08847,nw_src=10.10.3.100,nw_dst=10.10.4.100,dl_vlan=1,mp
root@PicOS-OVS#
```

The transmitted packet format to port te-1/1/2 is shown as follows (egress):



Configure Switch-C

In Switch-C, user needs to configure one flow which will SWAP the MPLS Label 10 to 100 for traffic RED.

```
root@PicOS-OVS# ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
device br0 entered promiscuous mode
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/1 vlan_mode=access tag=1 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/2 vlan_mode=access tag=1 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=1,dl_type=0x08847,nw_src=10.10.1.100,nw_dst=10.10.2.100,dl_vlan=1,mp
root@PicOS-OVS#
```

The transmitted packet format to port te-1/1/2 is shown as follows (egress):

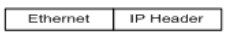


Configure Switch-D

In Switch-D, user needs to configure two flows, which will POP the MPLS Label 100 and 200 for traffic RED and BLUE, respectively.

```
root@PicOS-OVS# ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
device br0 entered promiscuous mode
root@PicOS-OVS#
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/1 vlan_mode=access tag=1 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/2 vlan_mode=access tag=1 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/3 vlan_mode=access tag=1 -- set Interface te-1/1/3 type=pica8
root@PicOS-OVS# ovs-vsctl add-port br0 te-1/1/4 vlan_mode=access tag=1 -- set Interface te-1/1/4 type=pica8
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=4,dl_type=0x08847,nw_src=10.10.1.100,nw_dst=10.10.2.100,dl_vlan=1,ac
root@PicOS-OVS#
root@PicOS-OVS# ovs-ofctl add-flow br0 in_port=3,dl_type=0x08847,nw_src=10.10.3.100,nw_dst=10.10.4.100,dl_vlan=1,ac
root@PicOS-OVS#
```

The transmitted packet format to port te-1/1/1 and te-1/1/2 is shown as follows (egress):



Multiple Virtual Bridges

In PicOS OVS, user can create multiple virtual bridges that are independent of one another. One physical port is able to add into only one virtual bridge. Each virtual bridge can be configured as a controller, respectively.

```
root@PicOS-OVS# ovs-vsctl  add-br br0 -- set bridge br0 datapath_type=pica8 other-config=datapath-id=0000d80aa99aaa
device br0 entered promiscuous mode
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/1 vlan_mode=access tag=1 -- set Interface te-1/1/1 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br0 te-1/1/2 vlan_mode=access tag=1 -- set Interface te-1/1/2 type=pica8
root@PicOS-OVS# ovs-vsctl  set-controller br0 tcp:10.10.50.1:6633
root@PicOS-OVS# ovs-vsctl  add-br br1 -- set bridge br1 datapath_type=pica8 other-config=datapath-id=0000d80bb99bbb
device br0 entered promiscuous mode
root@PicOS-OVS# ovs-vsctl  add-port br1 te-1/1/3 vlan_mode=access tag=1 -- set Interface te-1/1/3 type=pica8
root@PicOS-OVS# ovs-vsctl  add-port br1 te-1/1/4 vlan_mode=access tag=1 -- set Interface te-1/1/4 type=pica8
root@PicOS-OVS# ovs-vsctl  set-controller br1 tcp:10.10.50.2:6633
```

SSL Connection to Controller

If user wants to create an SSL connection with the controller in PicOS switch, please follow the following steps:

 # Switch

root@PicOS-OVS#**sudo apt-get install openssl**

Reading package lists... Done

Building dependency tree

Reading state information... Done

Suggested packages:

ca-certificates

The following NEW packages will be installed:

openssl

0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.

Need to get 696 kB of archives.

After this operation, 1070 kB of additional disk space will be used.

WARNING: The following packages cannot be authenticated!

openssl

Authentication warning overridden.

Get:1 http://ftp.debian.org/debian/ stable/main openssl powerpc 1.0.1e-2 [696 kB]

Fetched 696 kB in 5s (131 kB/s)

Selecting previously unselected package openssl.

(Reading database ... 17049 files and directories currently installed.)

Unpacking openssl (from .../openssl_1.0.1e-2_powerpc.deb) ...

Processing triggers for man-db ...

Setting up openssl (1.0.1e-2) ...

root@PicOS-OVS#ovs-pki init

/ovs/bin/ovs-pki: /ovs/var/lib/openvswitch/pki already exists and --force not specified

root@PicOS-OVS#**ovs-pki init --force**

Creating controllerca...

Creating switchca...

root@PicOS-OVS#**cd /ovs/var/lib/openvswitch/pki/controllerca**

root@PicOS-OVS#**ovs-pki req+sign ctl controller**

ctl-req.pem Mon Jan 13 03:26:05 UTC 2014

fingerprint 1cbf63b21301f33d9b4aa30540bff492f15bced3

root@PicOS-OVS#ls

ca.cnf careq.pem crl ctl-cert.pem ctl-req.pem index.txt.attr index.txt.old private serial.old

cacert.pem certs crlnumber ctl-privkey.pem index.txt index.txt.attr.old newcerts serial

root@PicOS-OVS#ls ctl-privkey.pem ctl-cert.pem

ctl-cert.pem ctl-privkey.pem

root@PicOS-OVS#**cd /ovs/var/lib/openvswitch/pki/switchca**

root@PicOS-OVS#**ovs-pki req+sign sc switch**

sc-req.pem Mon Jan 13 03:26:54 UTC 2014

fingerprint 65ed449bee94b8e7b8ba7da6f6584afd2f9cc2fb

root@PicOS-OVS#ls sc-privkey.pem sc-cert.pem

sc-cert.pem sc-privkey.pem

root@PicOS-OVS#

root@PicOS-OVS#**scp /ovs/var/lib/openvswitch/pki/controllerca/ctl-cert.pem 10.10.50.41:/home/build**

The authenticity of host '10.10.50.41 (10.10.50.41)' can't be established.

ECDSA key fingerprint is e6:04:3b:c8:24:36:c7:dd:c1:06:6a:69:e2:3b:82:2f.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.10.50.41' (ECDSA) to the list of known hosts.

root@10.10.50.41's password:

ctl-cert.pem 100% 4063 4.0KB/s 00:00

root@PicOS-OVS#**scp /ovs/var/lib/openvswitch/pki/controllerca/ctl-privkey.pem 10.10.50.41:/home/build**

root@10.10.50.41's password:

ctl-privkey.pem 100% 1675 1.6KB/s 00:00

root@PicOS-OVS#**scp /ovs/var/lib/openvswitch/pki/switchca/cacert.pem 10.10.50.41:/home/build**

root@10.10.50.41's password:

cacert.pem 100% 4028 3.9KB/s 00:00

root@PicOS-OVS#**ovs-vsctl set-ssl /ovs/var/lib/openvswitch/pki/switchca/sc-privkey.pem /ovs/var/lib/openvswitch/pki/switchca/sc-cert.pem /ovs/var/lib/openvswitch/pki/controllerca/cacert.pem**

root@PicOS-OVS#**ovs-vsctl del-br br0**

ovs-vsctl: no bridge named br0

root@PicOS-OVS#**ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8**

root@PicOS-OVS#**ovs-vsctl set-controller br0 ssl:10.10.50.41:6633**

root@PicOS-OVS#

 # Controllr

root@dev-41:/home/build# **ryu-manager --ctl-privkey ./ctl-privkey.pem --ctl-cert ./ctl-cert.pem --ca-certs ./cacert.pem --verbose**

loading app ryu.controller.ofp_handler

instantiating app ryu.controller.ofp_handler of OFPHandler

BRICK ofp_event

CONSUMES EventOFPPortDescStatsReply

CONSUMES EventOFPSwitchFeatures

CONSUMES EventOFPErrorMsg

CONSUMES EventOFPEchoRequest

CONSUMES EventOFPHello

connected socket:<eventlet.green.ssl.GreenSSLSocket object at 0x9f1ebfc> address:('10.10.50.155', 48508)

hello ev <ryu.controller.ofp_event.EventOFPHello object at 0x9ecf1ec>

move onto config mode

switch features ev version: 0x4 msg_type 0x6 xid 0xa2f1cf23 OFPSwitchFeatures(auxiliary_id=0,capabilities=7,datapath_id=746136833959685709 8L,n_buffers=256,n_tables=254)

move onto main mode

PICOS OpenFlow Tutorials

Basic Bridge Configuration

- Basic Bridge Introduction
- Power On Configuration
- Configure Switch
- Configure Bridge
- Configure Port
- Default Bridge Behavior
- OVS Commands Reference

Basic Flow Configurations

- Flow Introduction
- Modify Default Flow
- Uni-directional Flow
- 1-to-Many Multicasting
- Many-to-One Aggregation
- OVS Commands Used in this Tutorial
- Packet Address File

Connection to a RYU Controller

- RYU Introduction
- Introduce RYU Open Flow Controller
- Configure OVS for RYU OpenFlow Controller
- Controller-OVS Interaction
- RYU Simple Switch Application
- Open Flow Message Type
- RYU Guide OVS Commands Reference
- Using TTP (router profile) with RYU Controller

Connection to OpenDaylight Controller

- OpenDaylight Introduction
- Introduction to the OpenDaylight OpenFlow Controller
- Configure OVS for OpenDaylight Open Flow Controller
- OpenDaylight Controller-OVS Interaction
- OpenDaylight Simple Switch Application
- Message Type of Open Flow
- OVS Commands Reference 04

Connection to a Floodlight Controller

- Floodlight Controller Introduction
- Floodlight Open Flow Controller
- Test Topology
- Configure OVS
- Launch Floodlight
- Floodlight REST Interface

Configuration Guide for Atrium Stack on ONOS Controller

- ONOS Introduction
- Installation Guide
- ONOS Configuration Guide
- Quagga Configuration Guide
- PicOS Configuration Guide
- How to Install ONOS

Basic Bridge Configuration

- Basic Bridge Introduction
- Power On Configuration
- Configure Switch
- Configure Bridge
- Configure Port
- Default Bridge Behavior
- OVS Commands Reference

Basic Bridge Introduction

This document provides instructions on how to configure open switches running Pica8 PicOS software in various application scenarios. This document assumes minimal to no knowledge of OVS (Open vSwitch) and OpenFlow.

After studying this document, user will be able to configure OpenFlow on PicOS switches, know how to optimize the configuration for an application environment, and understand more about Open vSwitch and OpenFlow.

This document provides instructions for completing the following tasks:

- Configuring a PicOS switch as an OVS/OpenFlow switch.
- Creating bridges, adding ports, displaying bridge and port status/statistics, and displaying the OVS database.
- Configuring flow tables for uni-directional traffic, bi-directional traffic, traffic switching, one-to-many multicasting, mirroring, filtering, many-to-one aggregation etc.
- Configuring PicOS switches to connect with the Ryu controller

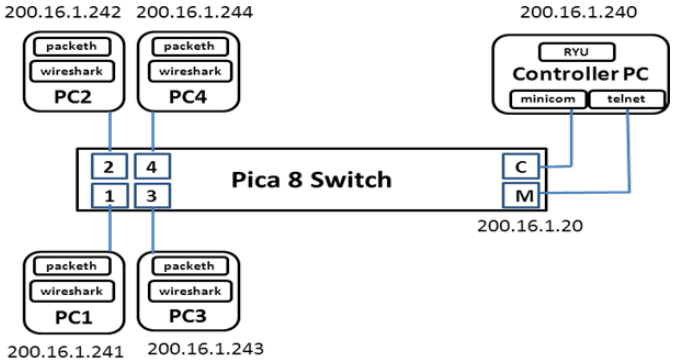


Figure 1 Test bed configuration

In this document, the system configuration depicted in Figure 1 includes:

- A Pica8 P-3295 open switch with 48 x 1GbE and 4 x 10GbE uplinks
- 5 Linux PCs running Ubuntu 12.4.1 LTS, one is connected to the management LAN port (RJ45) and console port (RJ45F); this PC is referred to the controller PC. The OpenFlow controller will be running on this PC. Four PCs are connected to 1GbE port 1 to 4 and serve as a data terminal for generating and monitoring traffic
- Tools installed on all the PCs are listed below. They can be installed through Linux installation utility *apt-get*
  - Terminal emulator minicom
  - Traffic monitoring tool Wireshark
  - Packet generator Packeth
  - ftp and ftpd

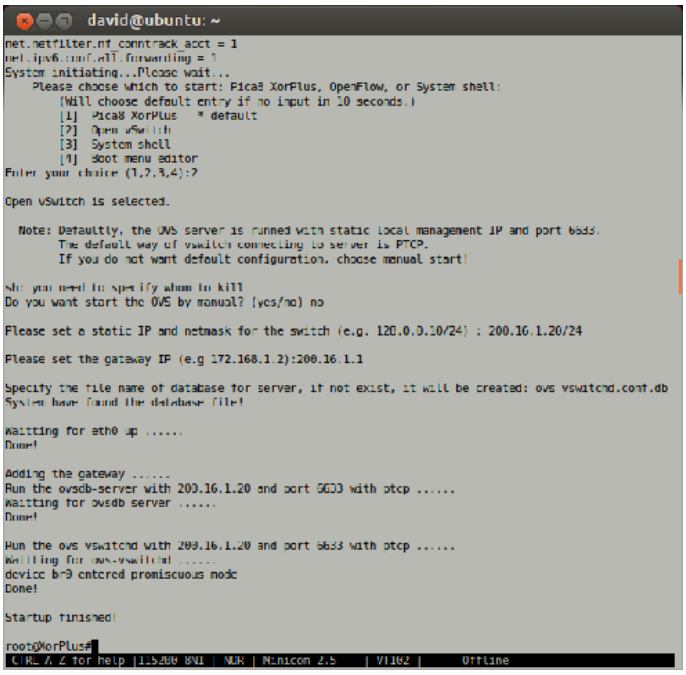
Power On Configuration

Connect with the console port of the PicOS switch as described in Initial Switch Access. Once the console connection is set up, power on the switch.

Figure 2 shows the console output. Do not not hit any keys until the booting choice menu appears. Enter ***2*** to boot into Open vSwitch mode. Next, the switch asks if the switch configuration should be done manually, enter ***no*** to enter the automatic mode. In this mode, the OVS processes will start automatically with default configuration such as log file, etc.

Next, the switch static IP address is entered. In this configuration, subnet 200.16.1.x is used. User can choose their own subnet address at this point. After the static IP address, a gateway IP address is entered. Next, an Open vSwitch configuration database name is required to store all the configuration information. In this example, *ovs-vswitchd.conf.db* database name is used. If the database name does not exist from previous configuration, it will be created in the default /ovs directory based on a database schema defined in /ovs/share/openvswitch/vswitch.ovsschema. Multiple databases can be created to provide different configurations; but only one database can be entered during this start up sequence. The OVS processes can be stopped and restarted manually, once the system is running. They can also be configured as cron processes. The database is persistent. The configuration stored in the database will be restored once the OVS processes start.

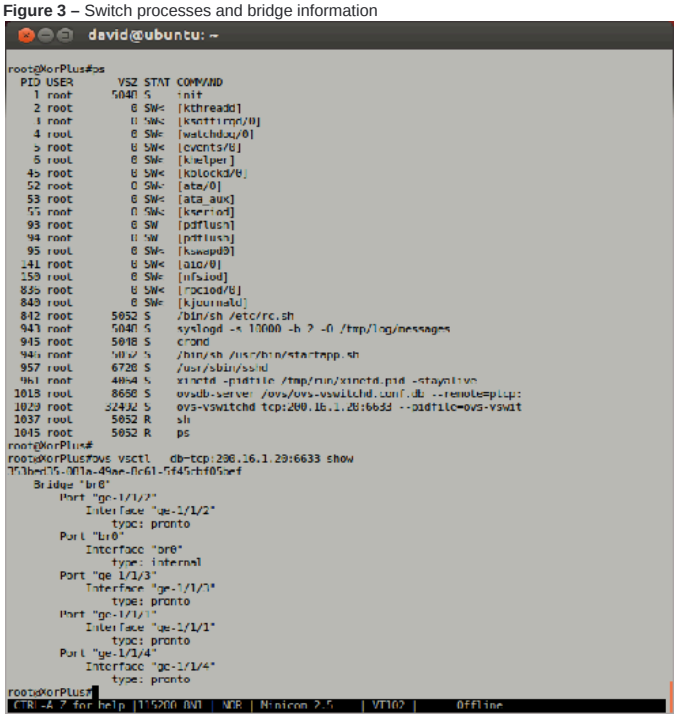
Figure 2 – Power on console output



In this example, the *ovs-vswitchd.conf.db* was used in a previous configuration. Therefore, the system found the database and created the initial configuration which will be shown later. In Figure 1, the management LAN port on the switch is *eth0. eth0* is connected to the *eth0* in the controller PC to allow the controller PC to *telnet* into the switch without the limitation of the console. In this configuration, all PCs are configured with static IP addresses to form an isolated environment for testing.

Next, the switch continues the boot sequence. Pay attention to the console messages regarding the *ovsdb-server* and *ovs-vswitchd*. They are the ovsdb server and ovs switch daemons. The IP address is the switch IP address and the 6633 is the default port number used to communicate with the ovs switch database server process. A different port number can be set through the manual configuration steps. Reference the PicOS Open vSwitch Configuration Guide for manual configuration steps.

Figure 3 – Switch processes and bridge information



The IP address and the port number is often used in the *ovs-vsctl* and *ovs-ofctl* commands discussed in later sections. The *ovs-vswitchd.conf.db* was used in a previous configuration, which contains a bridge *br0* with 4 1GbE ports. After the *ovs-vswitchd* process started, a message on *device br0* is shown to indicate the bridge has been created. At this point, the switch is up and running. The root level *root@PicOS-OVS#* shell prompt is shown and ready for user input. Multiple telnet windows can be started from the controller PC to login to the switch. The user id is *root* and the default password is *pica8.*

Configure Switch

Use Linux command ***ps -A*** to show the running processes. The *ovsdb-server* and *ovs-vswitchd* are there to indicate the ovs switch is ready for operation. Next, print the content of the switch database by using the ***ovs-vsctl show*** command to dump the switch configuration. It shows the database id, a bridge named *br0* with four 1GbE ports, and an internal port.

In most start up cases, a new database name of administrator's choice will be entered. As a result, an empty database is created. The show command will just show the database id. If a new database is created, the next step should be skipped, so move on to the *add-br* command. The following example will demonstrate how to delete the old bridge by utilizing the ***ovs-vsctl del-br br0*** command. Check the database content by using the show command which should just show the database id.The following example shows how to create a bridge and add ports for the bridge.

```
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
device br0 entered promiscuous mode
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/1 vlan_mode=trunk tag=1 -- set interface te-1/1/1 type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/2 vlan_mode=trunk tag=1 -- set interface te-1/1/2 type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/3 vlan_mode=trunk tag=1 -- set interface te-1/1/3 type=pica8
root@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/4 vlan_mode=trunk tag=1 -- set interface te-1/1/4 type=pica8
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl show
d4d12890-c07a-4303-80cc-c6f79cf3afd7
    Bridge "br0"
        Port "te-1/1/3"
            tag: 1
            Interface "te-1/1/3"
                type: "pica8"
        Port "te-1/1/4"
            tag: 1
            Interface "te-1/1/4"
                type: "pica8"
        Port "br0"
            Interface "br0"
                type: internal
        Port "te-1/1/2"
            tag: 1
            Interface "te-1/1/2"
                type: "pica8"
        Port "te-1/1/1"
            tag: 1
            Interface "te-1/1/1"
                type: "pica8"
root@PicOS-OVS$
```

Configure Bridge

To create a new bridge, issue ***ovs-vsctl add-br br0 – set bridge br0 datapath_type=pica8*** command. In the following example, the bridge needs four 1GbE ports. To add each 1GbE port to the bridge, issue ***ovs-vsctl add-port br0 ge-1/1/1 – set interface ge-1/1/1 type=pica8*** command 4 times to add ge-1/1/1 to ge1/1/4 to the bridge. To verify the configuration, use ***ovs-vsctl show*** to show the database content. As shown in the screen shot, the bridge should have four 1GbE ports and an internal port.
Next, monitor the port status and examine the port configuration with ***ovs-ofctl show br0*** command. The following commands are to show the configuration of the bridge.

```
root@PicOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2): dpid:5e3ec80aa9ae0a66
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x4):
1(te-1/1/1): addr:c8:0a:a9:ae:0a:66
config: 0
state: LINK_DOWN
current: FIBER
advertised: 1GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 0 Mbps now, 10000 Mbps max
2(te-1/1/2): addr:c8:0a:a9:ae:0a:66
config: 0
state: LINK_DOWN
current: FIBER
advertised: 1GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 0 Mbps now, 10000 Mbps max
3(te-1/1/3): addr:c8:0a:a9:ae:0a:66
config: 0
state: LINK_DOWN
current: FIBER
advertised: 1GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 0 Mbps now, 10000 Mbps max
4(te-1/1/4): addr:c8:0a:a9:ae:0a:66
config: 0
state: LINK_DOWN
current: FIBER
advertised: 1GB-FD FIBER
supported: 1GB-FD 10GB-FD FIBER AUTO_NEG
speed: 0 Mbps now, 10000 Mbps max
LOCAL(br0): addr:c8:0a:a9:ae:0a:66
config: 0
state: LINK_UP
current: 10MB-FD COPPER
supported: 10MB-FD COPPER
speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.4) (xid=0x6): frags=normal miss_send_len=0
root@PicOS-OVS$
root@PicOS-OVS$
root@PicOS-OVS$ovs-ofctl dump-ports br0
OFPST_PORT reply (OF1.4) (xid=0x2): 5 ports
port 1: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
tx pkts=0, bytes=0, drop=0, errs=0, coll=0
duration=228.085s
port 2: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
tx pkts=0, bytes=0, drop=0, errs=0, coll=0
duration=216.224s
port 3: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
tx pkts=0, bytes=0, drop=0, errs=0, coll=0
duration=208.941s
port 4: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
tx pkts=0, bytes=0, drop=0, errs=0, coll=0
duration=199.026s
port LOCAL: rx pkts=7, bytes=746, drop=0, errs=0, frame=0, over=0, crc=0
tx pkts=0, bytes=0, drop=0, errs=0, coll=0
duration=246.761s
```

```
root@PicOS-OVS$
```

In the example provided, port state is *LINKDOWN* because in the example set up, the cable has not been connected yet. The Pica8 1GbE port supports RJ45 copper connector and auto negotiation from 10 MB to 1 GB speed range. Next, examine the port statistics, using the _***ovs-ofctl dump-ports br0*** command. It shows the RX and TX statistics: since the link is down, no packets are sent or received, and all counters should be zeros.

Configure Port

A port can be added, deleted, turned up, or turned down, dynamically. The *add-port* command has been tested. To delete a port, use ***ovs-vsctl del-port br0 ge-1/1/1***. Port state can also be modified with the *mod−port* command ***ovs-ofctl mod-port br0 ge-1/1/1*** *action.* The keyword *action* can be one of the following parameters:

- Up or down

Enable or disable the interface. This is equivalent to *ifconfig up* or *ifconfig down* on a Linux system.

- Stp or no−stp

Enable or disable 802.1D spanning tree protocol (STP) on the interface. OpenFlow implementations that don't support STP will refuse to enable it.

- Receive or no−receive/receive−stp or no−receive−stp

Enable or disable OpenFlow processing of packets received on this interface. When packet processing is disabled, packets will be dropped instead of being processed through the OpenFlow table. The receive or no−receive setting applies to all packets except 802.1D spanning tree packets, which are separately controlled by receive−stp or no−receive−stp.

- Forward or no−forward

Allow or disallow forwarding of traffic to this interface. By default, forwarding is enabled.

- Flood or no−flood

Controls whether an OpenFlow flood action will send traffic out this interface. By default, flooding is enabled. Disabling flooding is primarily useful to prevent loops when a spanning tree protocol is not in use.

- packet−in or no−packet−in

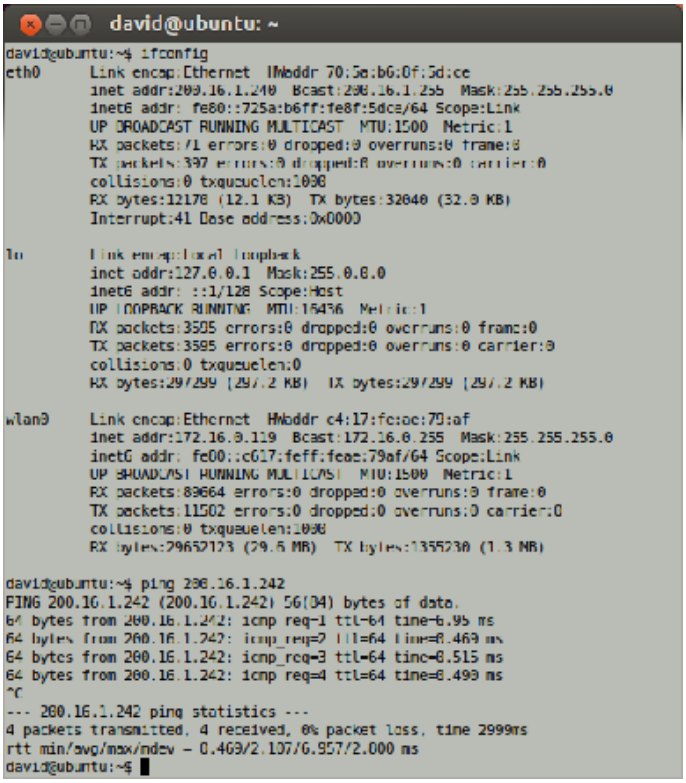
Controls whether packets received on this interface that do not match a flow table entry generate a "packet in" message to the OpenFlow controller. By default, "packet in" messages are enabled.

Again, the show command displays (among other information) the configuration that *mod−port* changes.

Default Bridge Behavior

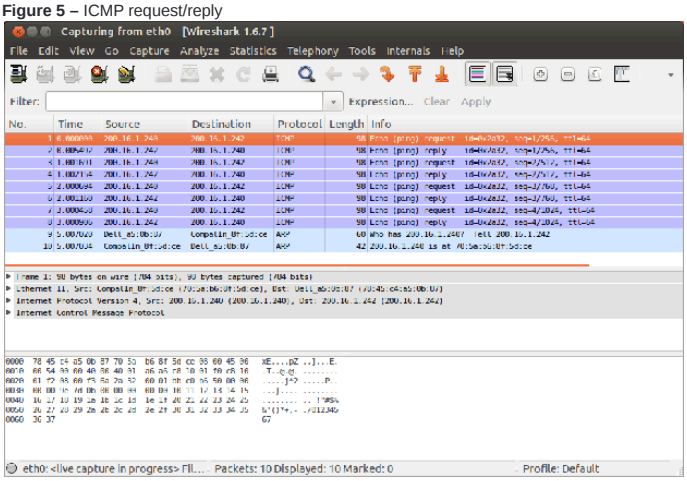
If the newly created bridge does not connect to the OpenFlow controller, it will behave as a simple L2 switch, which floods packets received from a port to all other ports. This behavior is implemented with a default low priority flow added at bridge creation time. The flow can be shown by using the **ovs-ofctl dump-flows br0** command. The flow will be shown as priority 0 and actions=NORMAL. Action NORMAL means the packet is subject to the device's normal L2/L3 processing. This action is not implemented by all OpenFlow switches. Next, connect 2 PCs to switch port 1 and port 2 with an Ethernet cable. Once the PCs are connected, the port state should be changed to LINK_UP soon after the cable is connected. Once both links are up, use ping to test the connectivity.

Figure 4 – Ping test



In this example, another Linux tool, wireshark, is also used to capture the packets sent and received on eth0. On the wireshark screen, a total of 4 pairs ping requests/replies are captured along with some arp packets. We can connect other PCs to the switch now, and ping should work for all PCs. In our set up, telnetd and ftpd are installed in our linux PC. User can try the telnet and ftp sessions to test the connectivity and bridge functionalities.

Figure 5 – ICMP request/reply



At this point, the switch is powered on, and the initial switch configuration without an open flow controller is completed. Proceed to Open SDN: Started Kit – Configure flows for flow manipulation.

OVS Commands Reference

```
ovs-vsctl  show
ovs-ofctl show br0
ovs-ofctl dump-ports br0
ovs-vsctl list-ports br0
ovs-vsctl list-ifaces br0
ovs-ofctl dump-flows br0
ovs-vsctl list-br
ovs-vsctl add-br br0 - set bridge br0 datapath_type=pica8
ovs-vsctl del-br br0
ovs-vsctl set Bridge br0 stp_enable=true
ovs-vsctl add-port br0 ge-1/1/1 - set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 - set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 - set interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 - set interface ge-1/1/4 type=pica8
ovs-vsctl add-port br0 ge-1/1/1 type=pronto options:link_speed=1G
ovs-vsctl del-port br0 ge-1/1/1
ovs-ofctl del-flows br0
```

Basic Flow Configurations

- Flow Introduction
- Modify Default Flow
- Uni-directional Flow
- 1-to-Many Multicasting
- Many-to-One Aggregation
- OVS Commands Used in this Tutorial
- Packet Address File

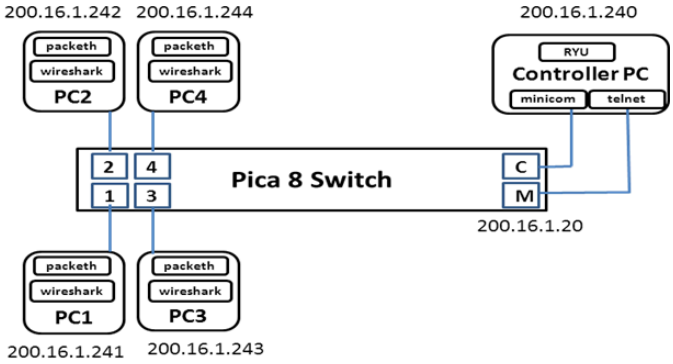
Flow Introduction

This document provides instructions on how to configure Pica8's open switches to work in various application scenarios. This document assumes the reader with minimal to no knowledge of the Open Virtual Switch (OVS) implementation defined by http://openvswitch.org/ or the OpenFlow protocol defined by https://www.opennetworking.org/. After studying this guide, user will have the tools needed to configure Pica8's open switches as an OpenFlow switch. User will also gain insights on how to optimize the configuration to work in an application environment, while also learning about OVS and the OpenFlow protocol.

This starter kit provides screen shots and a list of off-the-shelf applications needed to complete the configuration, as well as tips on problems user may encounter during setup. More documents or cookbooks on other subjects will be published periodically. This document provides a tutorial on how to:

- Configure a Pica8 switch as an OVS OpenFlow switch
- Create bridges; add ports; show bridge, port statistics, and status; introduction to the OVS database
- Configure flow tables for uni-directional, bi-directional, traffic switching, one-to-many multi-casting, mirroring, filtering, many-to-one aggregation, etc.
- Configure Pica8 OpenFlow switches to interface with the RYU OpenFlow Controller

Figure 1 – Test bed configuration



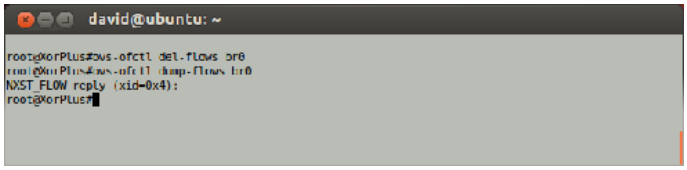
In this document, the system configuration depicted in Figure 1 includes:

- A Pica8 P-3295 open switch with 48 x 1 GbE and 4 x 10 GbE uplinks
- 5 Linux PCs running Ubuntu 12.4.1 LTS, one is connected to the management LAN port (RJ45) and console port (RJ45F). This PC is referred to the controller PC. The OpenFlow controller will be running on this PC. Four PCs are connected to 1GbE port 1 to 4 and serve as a data terminal for generating and monitoring traffic
- Tools installed on all the PCs are listed below. They can be installed through Linux installation utility *apt-get*
  - Terminal emulator minicom
  - Traffic monitoring tool Wireshark
  - Packet generator Packeth
  - ftp and ftpd

Modify Default Flow

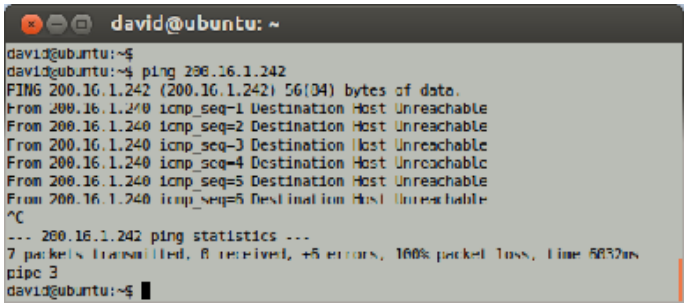
Next, the process of disabling flooding behavior, starting configuration of flow table, and manipulating packet flows will be shown. Use the ***ovs-ofctl del-flows br0*** command to delete the default flow. Dump the flow table, and no flow entry is shown.

Figure 2 – Delete flows and dump flows



At this point, the ping should stop working because the flooding has been disabled. If interested, user can delete the bridge and re-create it with four ports. Then, the ping should work again.

Figure 3 – Pings



Uni-directional Flow

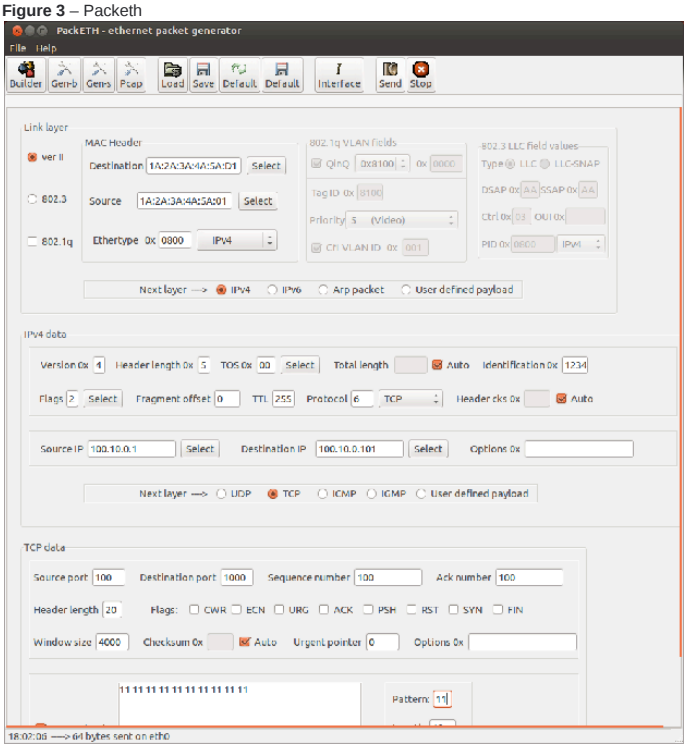
Before running uni-directional flow, user needs a packet generator to work with *wireshark* for packet generation and capturing. In this starter kit, a linux tool *packeth* is used for packet generation. The *packeth* can be installed via the linux command *sudo apt-get install packeth*. To use the *packeth*, an address file needs to be created as the address database for packet creation. The format is <IP address>:<MAC address>:<Names>. A sample address file is provided in the appendix Packet Address File.

Next, user can create some packets to be used in the later test scenarios. Start the *packeth*, click the *builder* button to enter the tab for creating a packet. The next screen shows the test packet we built for this test. Fill in each field using the *select* button or by entering the value. Each packet includes information in link layer, IP layer, and TCP payload. Once the packet is built, click the *interface* button then select *eth0* as the interface.

Next, create a uni-directional flow from port 1 to port 2 using ***ovs-ofctl add-flow br0 in_port=1,actions=output:2*** command. Then, use the dump flow command to show the flow. The command added a flow into *br0* to forward all packets coming in from *in_port=1* to *out_port=2*. Next, start the *wireshark* application to capture all packets on *eth0* for both PC1 and PC2.

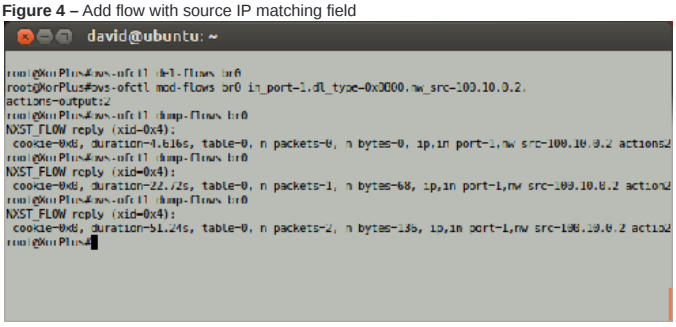
Next, return to the *packeth* screen and click the *send* button. At the bottom of the *packeth* screen, there should be a time stamp and the number of bytes sent to eth0 shown. User can verify the packet content on *wireshark* on both the sending and receiving PCs. This verifies the flow entry entered via the *add-flow* command works as expected. To test this flow further, follow the next *packeth* screen to create another packet with different information and send it through the *eth0*.

Figure 3 – Packeth



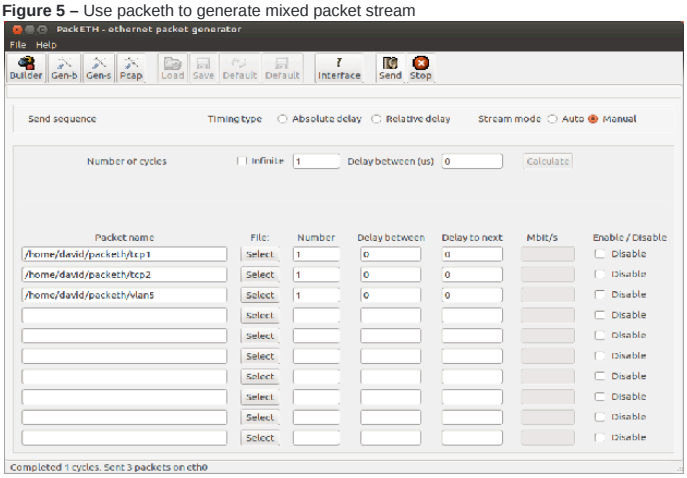
Next, use *ovs-ofctl del-flows br0* command to delete the flow. Then, use *ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.2,actions=output:2* to add a new flow that filters all packets received from port 1 and only forwards the packets with the matching IP address to port 2.

Figure 4 – Add flow with source IP matching field



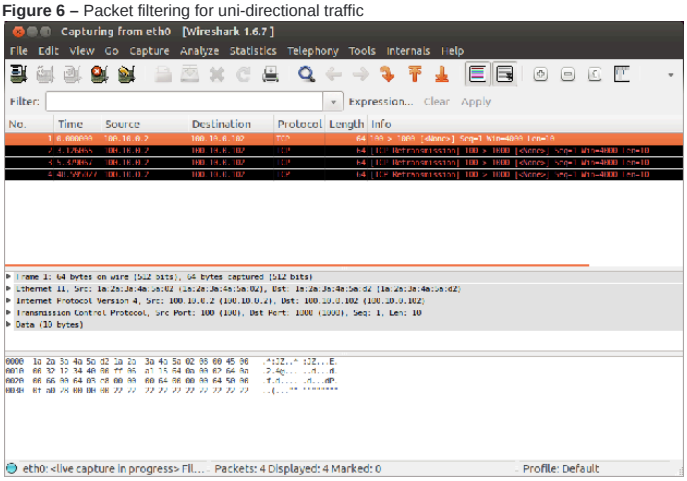
On the *packeth* menu, click the *gen-s* button to mix packets into one output stream. Select different packets built with different IP addresses to form one packet stream. Specify the delay and number of iteration. Then, select the manual operation to send the stream. Use *wireshark* to examine the result.

Figure 5 – Use packeth to generate mixed packet stream



As shown in the screen shot, the packet stream sent using *packeth,* with 3 different types of the packet and 3 different source IP addresses, is filtered by the flow and only the packet with source IP address 100.10.0.2 is forwarded to output port 2. With the *packeth* and *wireshark*, many of the fields can be tested in the uni-directional flow configuration.

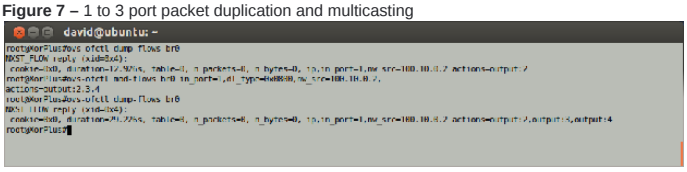
Figure 6 – Packet filtering for uni-directional traffic



1-to-Many Multicasting

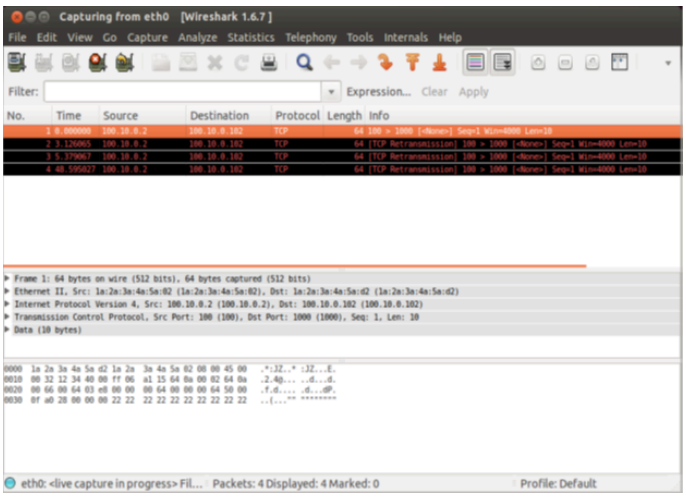
After the unidirectional flow from one port to another, modify the flow entry to configure a 1-to-3 ports multicasting scenario where packets matching the flow entry are duplicated and forwarded to 3 output ports. This time, use the *mod-flows* command ***ovs-ofctl mod-flows br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.2,actions=output:2,3,4***. Then, use the dump flow command to verify the flow is set up correctly.

Figure 7 – 1 to 3 port packet duplication and multicasting



Configure the *packeth* and *wireshark* on all PCs, send the packets into port 1, and examine the packets received on port 2, 3, and 4 to see if the action matches the flow specification.

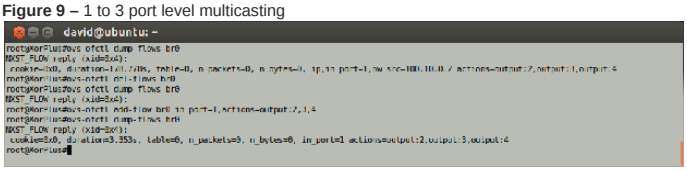
Figure 8 – 1 to 3 port packet filtering, duplication, and multicasting



Next, use the *packeth* to build packet with VLAN, priority, ARP, TCP, UDP, and ICMP packets to exercise various flow packet matching fields and use the *wireshark* to verify the output.

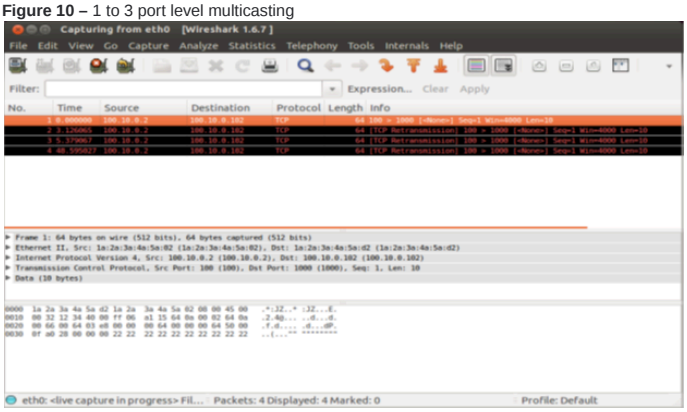
In addition to using filters in multicasting, port level duplication and multicasting is also supported. To configure this scenario, first clean up the flows in *br0* using *ovs-ofctl del-flows br0*. Then, use *ovs-ofctl add-flow br0 in_port=1,actions=output:2,3,4* to add a new multicasting flow.

Figure 9 – 1 to 3 port level multicasting



The same traffic with source IP 100.10.0.2 is sent to port 1. The received traffic on port 4 is captured using *wireshark*. With the tools described in this document, various traffic patterns combined with different filters can be configured to test application scenarios.

Figure 10 – 1 to 3 port level multicasting

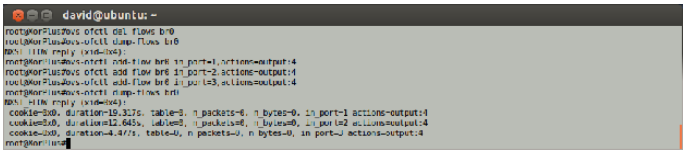


Many-to-One Aggregation

In this section, flow aggregation from multiple ports is examined. Two scenarios will be configured. The first scenario is to aggregate traffic from port 1, 2, and 3 without any filtering to port 4. The second scenario is to apply packet matching filter on each port to select specific traffic based on source IP address from each port for aggregation. For the first scenario, delete the existing flows using the ***ovs-ofctl del-flows br0*** command. Then, use the following commands to add 3 flows to the flow table:

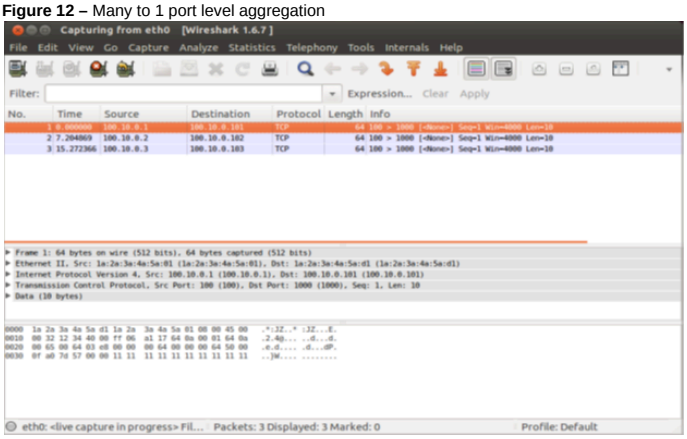
- *ovs-ofctl add-flow br0 in_port=1,actions=output:4*
- *ovs-ofctl add-flow br0 in_port=2,actions=output:4*
- *ovs-ofctl add-flow br0 in_port=3,actions=output:4*

Figure 11 – Many to 1 port level aggregation



Configure *packeth* on each PC to send packets from port 1 to 3, with source IP 100.10.0.1 from port1, source IP 100.10.0.2 from port 2, and 100.10.0.3 from port 3. All the packets should be forwarded to port 4.

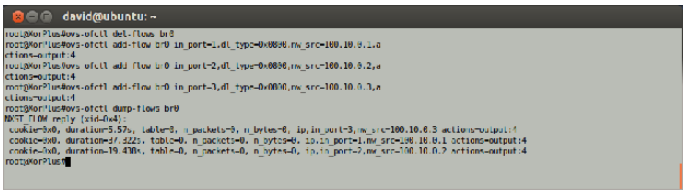
Figure 12 – Many to 1 port level aggregation



In this many-to-one aggregation configuration, if the aggregated traffic is more than 1 Gbps, the over-subscribed packets will be dropped. The over-subscription scenario could not be demonstrated in this set up because the PC only has a 100 Mbps Ethernet port. But if user can create the scenario, the dropped packets can be shown via the ***ovs-ofctl dump-ports br0*** command as part of the port counters.
To engineer the traffic aggregation, the filters described in *Open SDN: Starter kit – Power on and configure switch* can be applied to identify and select traffic for aggregation. In the scenario below, three flows are created with a filter on separate IP address on each port. The previous flows need to be deleted first, then use the following commands to set up the new flows:

- *ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.1,actions=output:4*
- *ovs-ofctl add-flow br0 in_port=2,dl_type=0x0800,nw_src=100.10.0.2,actions=output:4*
- *ovs-ofctl add-flow br0 in_port=3,dl_type=0x0800,nw_src=100.10.0.3,actions=output:4*

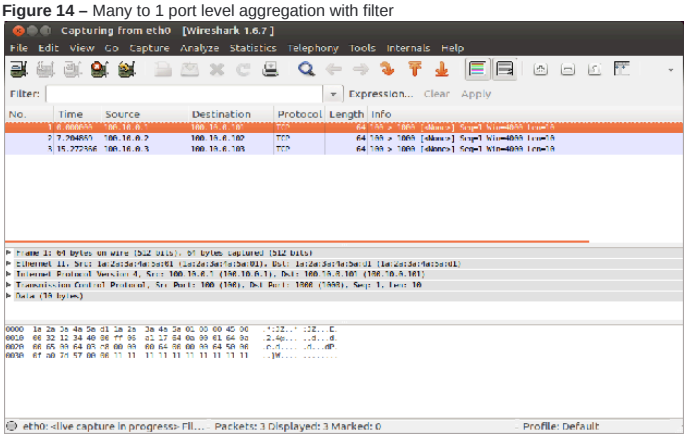
Figure 13 – Many to 1 port level aggregation



The *packeth* is configured to generate traffic with mixed source IP addresses. Try this with a manual option first to send a small amount of traffic through each port. Then, monitor the traffic on *wireshark* to see if the packets are filtered and forwarded correctly.

The *dump-flows* command is handy to verify the number of packets matched by the filtering rule. The ***ovs-ofctl dump-ports br0*** command is also very useful to show all the port statistics. Flows can be modified dynamically based on traffic conditions to throttle traffic during over-subscription, provide load balance, and re-distribute traffic. In deployment scenario, flows are managed via Open Flow controller with Open Flow protocols. In the next Starter kit, the RYU Open Flow controller will be discussed to show the controller-switch interaction.

Figure 14 – Many to 1 port level aggregation with filter



OVS Commands Used in this Tutorial

```
ovs-vsctl show
ovs-ofctl show br0
ovs-ofctl dump-ports br0
ovs-vsctl list-br
ovs-vsctl list-ports br0
ovs-vsctl list-ifaces br0
ovs-ofctl dump-flows br0
ovs-ofctl snoop br0
ovs-vsctl add-br br0 - set bridge br0 datapath_type=pica8
ovs-vsctl del-br br0
ovs-vsctl set-controller br0 tcp:172.16.1.240:6633
ovs-vsctl del-controller br0
ovs-vsctl set Bridge br0 stp_enable=true
ovs-vsctl add-port br0 ge-1/1/1 - set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 - set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 - set interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 - set interface ge-1/1/4 type=pica8
ovs-vsctl add-port br0 ge-1/1/1 type=pronto options:link_speed=1G
ovs-vsctl del-port br0 ge-1/1/1
ovs-ofctl add-flow br0 in_port=1,actions=output:2
ovs-ofctl mod-flows br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.1,actions=output:2
ovs-ofctl add-flow br0 in_port=1,actions=output:2,3,4
ovs-ofctl add-flow br0 in_port=1,actions=output:4
ovs-ofctl del-flows br0
ovs-ofctl mod-port br0 1 no-flood
ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=192.168.1.241,actions=output:3
ovs-ofctl add-flow br0 in_port=4,dl_type=0x0800,dl_src=60:eb:69:d2:9c:dd,nw_src=198.168.1.2,nw_dst=124.12.123.55,a
ovs-ofctl mod-flows br0 in_port=4,dl_type=0x0800,nw_src=192.210.23.45,actions=output:3
ovs-ofctl del-flows br0 in_port=1
```

Packet Address File

```
100.10.0.1,1a:2a:3a:4a:5a:01,stream1
100.10.0.2,1a:2a:3a:4a:5a:02,stream2
100.10.0.3,1a:2a:3a:4a:5a:03,stream3
100.10.0.4,1a:2a:3a:4a:5a:04,stream4
100.10.0.5,1a:2a:3a:4a:5a:05,stream5
100.10.0.6,1a:2a:3a:4a:5a:06,stream6
100.10.0.7,1a:2a:3a:4a:5a:07,stream7
100.10.0.8,1a:2a:3a:4a:5a:08,stream8
100.10.0.9,1a:2a:3a:4a:5a:09,stream9
100.10.0.10,1a:2a:3a:4a:5a:0a,stream10
100.10.0.101,1a:2a:3a:4a:5a:d1,stream101
100.10.0.102,1a:2a:3a:4a:5a:d2,stream102
100.10.0.103,1a:2a:3a:4a:5a:d3,stream103
100.10.0.104,1a:2a:3a:4a:5a:d4,stream104
100.10.0.105,1a:2a:3a:4a:5a:d5,stream105
100.10.0.106,1a:2a:3a:4a:5a:d6,stream106
100.10.0.107,1a:2a:3a:4a:5a:d7,stream107
100.10.0.108,1a:2a:3a:4a:5a:d8,stream108
100.10.0.109,1a:2a:3a:4a:5a:d9,stream109
100.10.0.110,1a:2a:3a:4a:5a:da,stream110
```

Connection to a RYU Controller

In a software-defined network, the Ryu controller is used to manage how traffic is handled. Ryu provides APIs intended to make it easy for developers to write network management and control applications used in an SDN. Using Ryu, organizations can create customized applications for managing and controlling their networks. They can also modify existing components. In either case, the applications communicate to the Ryu controller, delivering instructions on how network traffic should be managed. Ryu supports OpenFlow and other protocols (including Netconf and OF-config) to interact with the forwarding plane and dictate traffic flows. It works with Open vSwitch switches, including switches based on Pica8 PICOS.

This document describes how to configure Ryu controllers in PICOS.

- RYU Introduction
- Introduce RYU Open Flow Controller
- Configure OVS for RYU OpenFlow Controller
- Controller-OVS Interaction
- RYU Simple Switch Application
- Open Flow Message Type
- RYU Guide OVS Commands Reference
- Using TTP (router profile) with RYU Controller

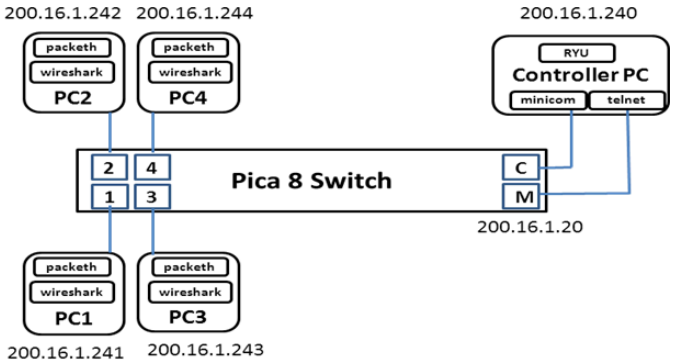
RYU Introduction

This document provides instructions on how to configure Pica8's open switches to work in various application scenarios. This document assumes the reader with minimal to no knowledge of the Open Virtual Switch (OVS) implementation defined by http://openvswitch.org/ or the OpenFlow protocol defined by https://www.opennetworking.org/. After studying this guide, user will have the tools needed to configure Pica8's open switches as an OpenFlow switch. User will also gain insights on how to optimize the configuration to work in an application environment while also learning about OVS and the OpenFlow protocol.

This starter kit provides screen shots and a list of off-the-shelf applications needed to complete the configuration, as well as tips regarding problems user may encounter during the setup. More documents or cookbooks on other subjects will be published periodically. This document provides a tutorial on how to:

- Configure Pica8 as an OVS OpenFlow switch
- Create bridges, add ports, show bridge and port statistics, status, as well as the OVS database
- Configure flow tables for uni-directional, bi-directional, traffic switching, one-to-many multi-casting, mirroring, filtering, many-to-one aggregation, etc.,
- Configure Pica8 OVS OpenFlow switches to interface with the RYU OpenFlow Controller

Figure 1 – Test bed configuration



In this document, the system configuration depicted in Figure 1 includes:

- A Pica8 P-3295 open switch with 48 x 1 GbE and 4 x 10 GbE uplinks
- 5 Linux PCs running Ubuntu 12.4.1 LTS, one is connected to the management LAN port (RJ45) and console port (RJ45F); this PC is referred to the controller PC. The OpenFlow controller will be running on this PC. Four PCs are connected to 1GbE port 1 to 4 and serve as a data terminal for generating and monitoring traffic
- Tools installed on all the PCs are listed below. They can be installed through Linux installation utility *apt-get*
    - Terminal emulator minicom
    - Traffic monitoring tool Wireshark
    - Packet generator Packeth
    - ftp and ftpd

Introduce RYU Open Flow Controller

RYU is an open flow controller that has been integrated with the Pica8 open switch with OVS 1.10 implementation that supports Open Flow v1.3. Additional RYU information can be found at the RYU website http://osrg.github.com/ryu/. The purpose of Pica8 RYU integration is to provide an open source SDN platform so that the SDN community can prototype, test, and develop applications in an open source environment with an open flow switching platform for real traffic testing. With the configuration provided in this starter kit, user should be able to have real traffic running in a week to test out the application scenarios using OVS commands. Both OVS and RYU are open source with Apache licenses that developers can access easily.

To clone the RYU directory, open a shell window from $home directory. Then, use *git clone git://github.com/osrg/ryu.git* to copy the RYU code base. It will create an *ryu* directory in $home.

Figure 2 – Clone RYU. Then *cd ryu* and *sudo python ./setup.py install* to complete the installation.

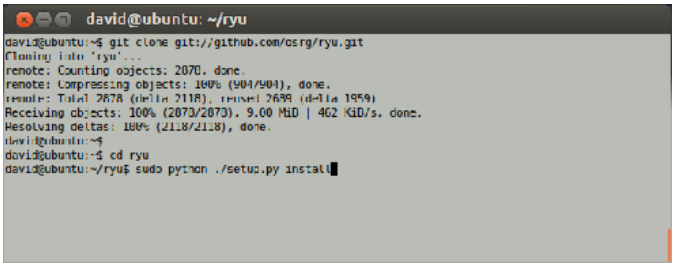


Figure 3 – Install RYU. The installation installs the *ryu-manager* and *ryu-client* to the $home/*ryu/bin* and */usr/local/bin* directories. Now we are ready to run the test applications.

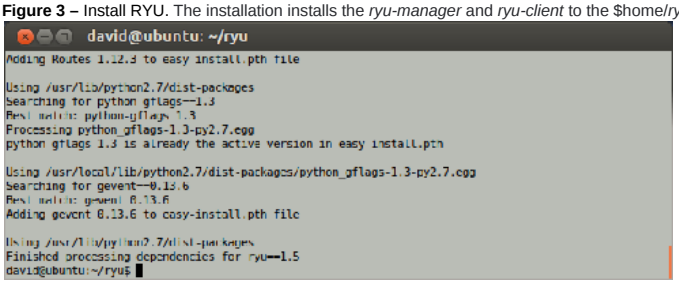
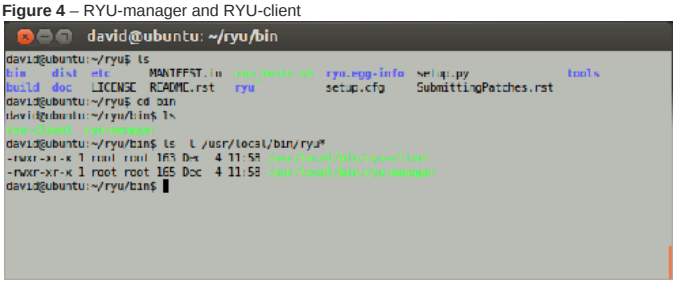


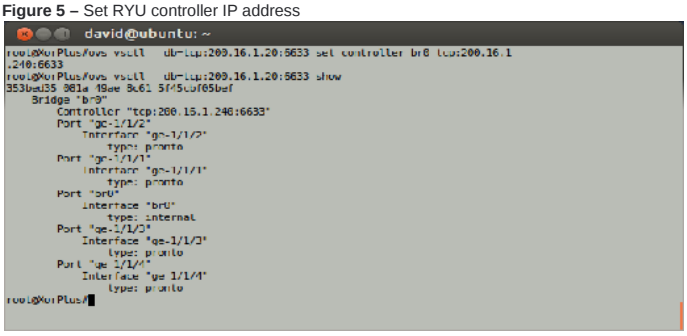
Figure 4 – RYU-manager and RYU-client



Configure OVS for RYU OpenFlow Controller

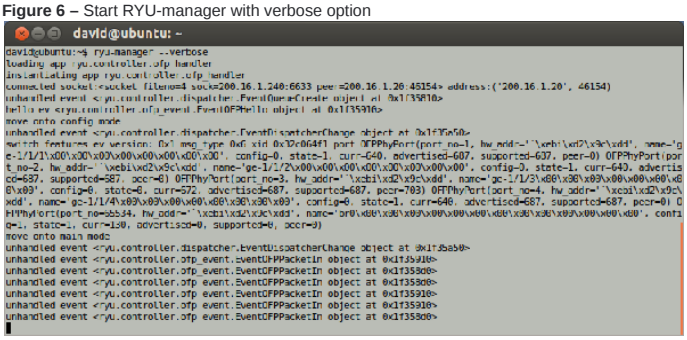
In OVS, the controller property of the bridge created earlier needs to be added to include the controller IP address and port number. The command ***ovs-vsctl set-controller br0 tcp:200.16.1.240:6633*** sets the controller address for bridge *br0* on port 6633. The command ***ovs-vsctl show*** would then show the bridge information. The connection status is not shown because the controller has not been started yet.

Figure 5 – Set RYU controller IP address



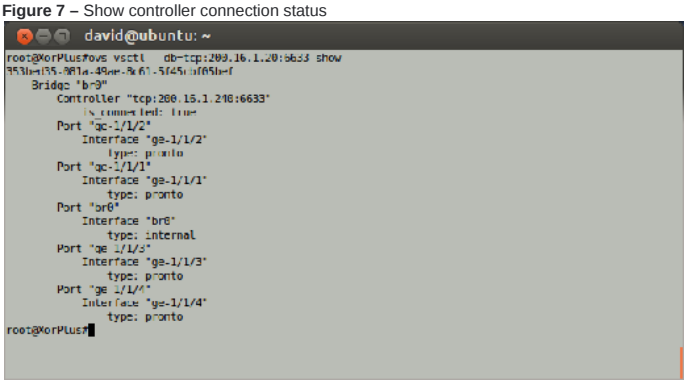
The RYU controller will be running on the controller PC with IP address 200.16.1.240 using the default port 6633. The port number can be changed. For this exercise, the controller will be started with the *–verbose* mode.

Figure 6 – Start RYU-manager with verbose option



The *--verbose mode* helps us understand the *RYU controller-OVS* interaction. Use the command ***ryu-manager* –verbose** to start the controller. The TCP connection is established first and the connection information is printed with peer (OVS) IP address 10.10.50.20. Once the controller is started, the connection status will change to *is_connected: true*. The controller port information can also be shown using the command ***ovs-ofctl show*** *br0*.

Figure 7 – Show controller connection status

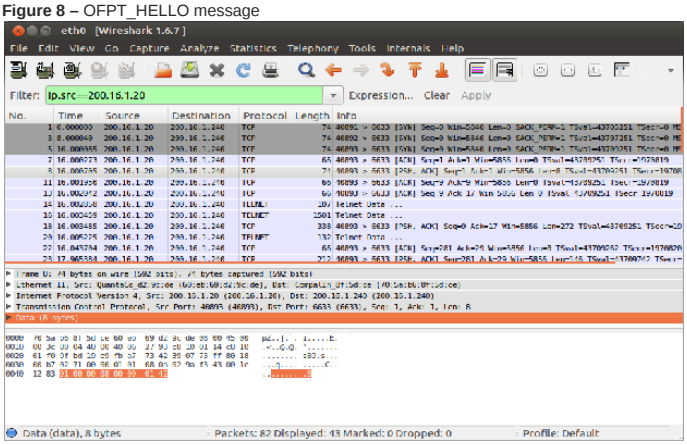


Controller-OVS Interaction

Once the controller and OVS are connected, a set of messages will be exchanged. For example, the OVS sends an OFPT_HELLO message to the controller. The hello message is captured on the *wireshark* screen. The first byte of the message is the version number and the second byte is the OFPT_TYPE. OFTP_HELLO message is type 0.

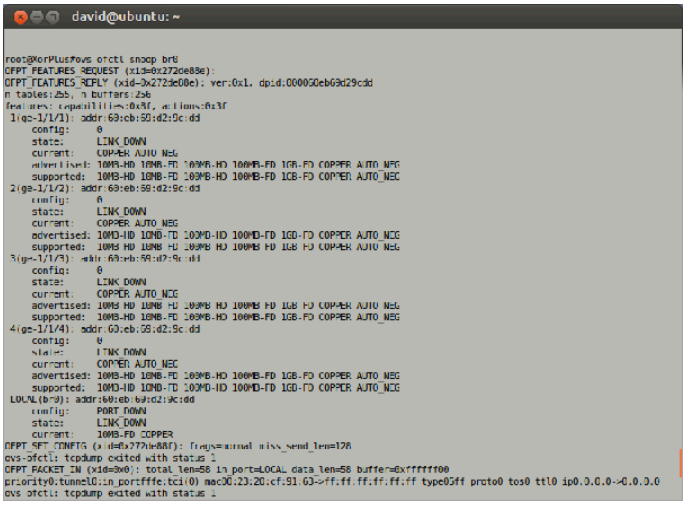
After the hello message from the switch, the controller sends OFPT_FEATURES_REQUEST (type=5) to retrieve the switch capabilities, including the supported open flow version, switch configuration, port hardware address, etc. The switch sends OFPT_FEATURES_REPLY (type=6) to provide the feature information. The message is shown on both the controller console and switch console.

Figure 8 – OFPT_HELLO message



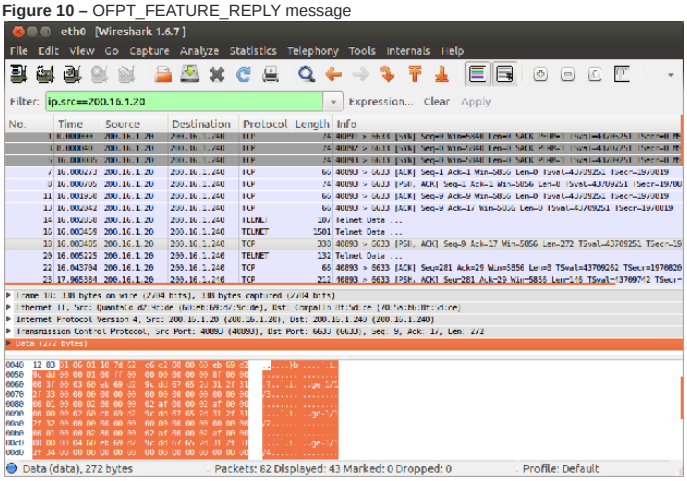
The switch console information is provided by the snoop option of the *ovs-ofctl* command. The command is ***ovs-ofctl snoop br0.*** It shows the feature request from the controller and the feature reply with the bridge information. User can compare the switch console information with the controller console information to get a better understanding of the message exchange.

Figure 9 – ovs-ofctl snoop br0



The *wireshark* also captured the information. Notice the message type in the second byte is 6 representing the OFPT_FEATURES_REPLY. After the feature reply, the controller sends an OFPT_SET_CONFIG message to set the message parameters such as max length, etc. Once the controller is connected, the OVS changes its default behavior from a layer 2 switch to an OVS switch. It means the flooding is disabled and open flow packet processing starts. Each packet is processed based on the flow table entry. Unmatched packets are forwarded to the controller for analysis unless a rule is defined to drop the packet.
During initial start up with the controller, the flow table is empty. Therefore, packets received from any port are forwarded to the controller. The next message from the switch is type OFPT_PACKET_IN (type=10/0x0a).

Figure 10 – OFPT_FEATURE_REPLY message

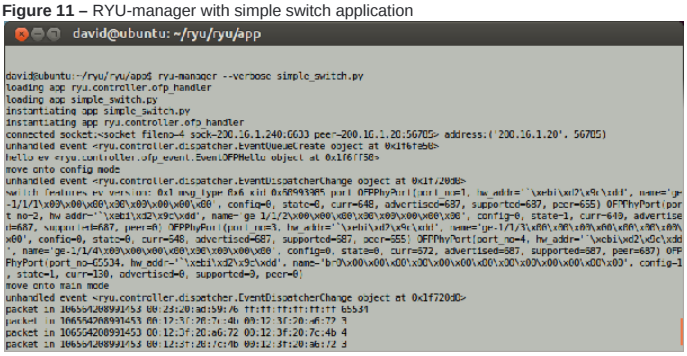


In this exercise, the *RYU-manager* does not have any application to receive and process the OFPT_PACKET_IN message. Therefore, on the controller screen, a bunch of *unhandled_events* are printed on the console. At this point, the RYU-OVS open flow session is established and ready for Open Flow application to take over the event handling and flow configuration.

RYU Simple Switch Application

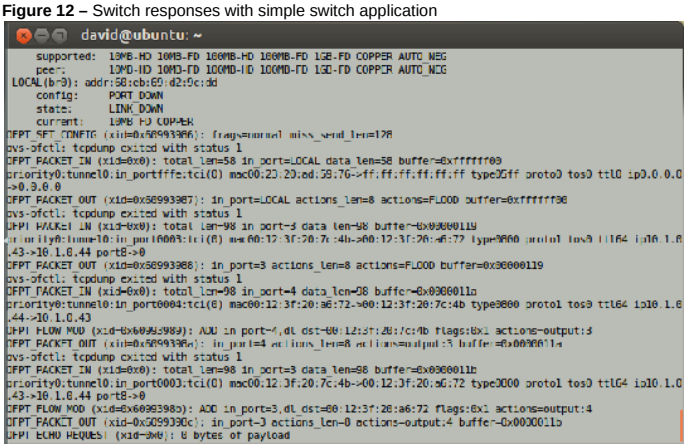
With just the controller connected without any application, the ping between the PCs cannot work because the ARP requests are forwarded to the controller without any packet processing instructions in the flow tables. RYU code distribution comes with a set of applications to show how applications can be integrated. The following instructions will show how to run the simple switch application. The application processes the *packet_in* messages (e.g., ICMP_REQUEST) and instructs the bridge to flood all other ports with the packets once the destination host has received the request and has replied with its MAC address. This simple switch application sets up the flow table to forward traffic from source port to the correct destination port. This is the default switch behavior that we have tested before. The application is in the $home/ryu/ryu/application directory. Run the *ryu-manager –verbose simple_switch.py* command to start the application.

Figure 11 – RYU-manager with simple switch application



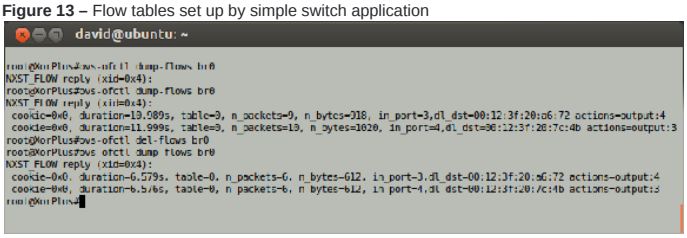
Once the simple switch application starts, the first part of the message output is the same as before, but instead of receiving unhandled events only as the previous RYU-manager only run, it sends an OFPT_PACKET_OUT message to the switch with FLOOD actions on first two packet_in messages. The first one is a probe message sent by the controller on local port.

Figure 12 – Switch responses with simple switch application



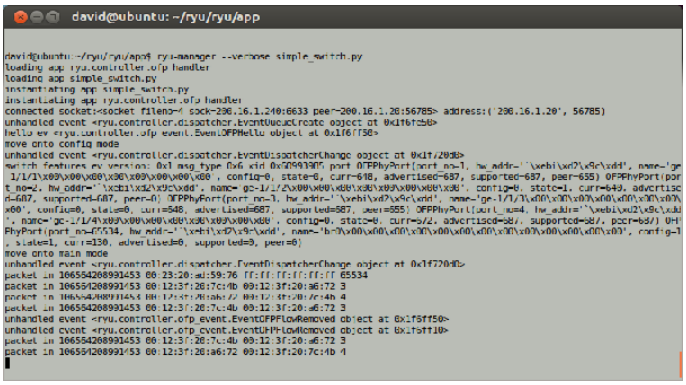
The second message is an ICMP request that comes in from port 3 and has a target destination of port 4. This message is the result of a ping test running on the PC connected to port 3 to PC on port 4. Since the controller does not know which port has the PC 4 MAC address. It sends the OFPT_PACKET_OUT instruction to the switch to flood the message received on port 3. Once the PC on port 4 receives the ICMP request, it responds with its reply. The controller matches the reply destination MAC address with the PC3 on port3 and sends an OFPT_FLOW_MOD action to create a flow from port 4 to port 3 to forward the packets. The same process repeats again for setting up flows from port 3 and port 4.

Figure 13 – Flow tables set up by simple switch application



As a result, the *dump-flows* show 2 flows created by the simple switch application. To test it again, simply use *del-flows* command to delete the flow.

Figure 14 – Delete flow event from switch to controller



Once the flows are deleted, two OPEN_FLOW_REMOVED events are generated by the switch to notify the controller. The MAC learning process repeats itself again. The two flows will be created when the next round of the ICMP requests come into the controller. User can dump the flow table to verify its behavior. At this point, the starter kit has demonstrated the basic RYU controller integration with OVS and a simple application built on top of the RYU controller. Reader should be able to start testing and writing test applications using the SDN platform presented in this document.

Open Flow Message Type

```
# enum ofp_type
OFPT_HELLO = 0 # Symmetric message
OFPT_ERROR = 1 # Symmetric message
OFPT_ECHO_REQUEST = 2 # Symmetric message
OFPT_ECHO_REPLY = 3 # Symmetric message
OFPT_VENDOR = 4 # Symmetric message
OFPT_FEATURES_REQUEST = 5 # Controller/switch message
OFPT_FEATURES_REPLY = 6 # Controller/switch message
OFPT_GET_CONFIG_REQUEST = 7 # Controller/switch message
OFPT_GET_CONFIG_REPLY = 8 # Controller/switch message
OFPT_SET_CONFIG = 9 # Controller/switch message
OFPT_PACKET_IN = 10 # Async message
OFPT_FLOW_REMOVED = 11 # Async message
OFPT_PORT_STATUS = 12 # Async message
OFPT_PACKET_OUT = 13 # Controller/switch message
OFPT_FLOW_MOD = 14 # Controller/switch message
OFPT_PORT_MOD = 15 # Controller/switch message
OFPT_STATS_REQUEST = 16 # Controller/switch message
OFPT_STATS_REPLY = 17 # Controller/switch message
OFPT_BARRIER_REQUEST = 18 # Controller/switch message
OFPT_BARRIER_REPLY = 19 # Controller/switch message
OFPT_QUEUE_GET_CONFIG_REQUEST = 20 # Controller/switch message
OFPT_QUEUE_GET_CONFIG_REPLY = 21 # Controller/switch message
```

RYU Guide OVS Commands Reference

```
ovs-vsctl show
ovs-ofctl show br0
ovs-ofctl dump-ports br0
ovs-vsctl list-br
ovs-vsctl list-ports br0
ovs-vsctl list-ifaces br0
ovs-ofctl dump-flows br0
ovs-ofctl snoop br0
ovs-vsctl add-br br0 - set bridge br0 datapath_type=pica8
ovs-vsctl del-br br0
ovs-vsctl set-controller br0 tcp:172.16.1.240:6633
ovs-vsctl del-controller br0
ovs-vsctl set Bridge br0 stp_enable=true
ovs-vsctl add-port br0 ge-1/1/1 - set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 - set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 - set interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 - set interface ge-1/1/4 type=pica8
ovs-vsctl add-port br0 ge-1/1/1 type=pronto options:link_speed=1G
ovs-vsctl del-port br0 ge-1/1/1
ovs-ofctl add-flow br0 in_port=1,actions=output:2
ovs-ofctl mod-flows br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.1,actions=output:2
ovs-ofctl add-flow br0 in_port=1,actions=output:2,3,4
ovs-ofctl add-flow br0 in_port=1,actions=output:4
ovs-ofctl del-flows br0
ovs-ofctl mod-port br0 1 no-flood
ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=192.168.1.241,actions=output:3
ovs-ofctl add-flow br0 in_port=4,dl_type=0x0800,dl_src=60:eb:69:d2:9c:dd,nw_src=198.168.1.2,nw_dst=124.12.123.55,actions=output:1
ovs-ofctl mod-flows br0 in_port=4,dl_type=0x0800,nw_src=192.210.23.45,actions=output:3
ovs-ofctl del-flows br0 in_port=1
```

Using TTP (router profile) with RYU Controller

A Table Type Pattern (TTP) is an Open Network Foundation (ONF) effort to more easily enable an OpenFlow controller and switch to agree on a set of functionalities during configuration. A TTP describes specific forwarding behaviors that an OpenFlow controller can program using the OpenFlow-Switch protocol.

With respect to the Pica8 PICOS network operating system and white box switches, TTPs help overcome the limitations of Ternary Content Addressable Memory (TCAM) devices. TCAMs are power hungry, expensive memory devices that bloat the cost of solutions and cannot scale well. TTPs enable OpenFlow access to other ASIC tables, such as the VLAN, MAC, and IP along with TCAM tables. As the NOS opens up the different tables in the ASIC, an OpenFlow application is able to control the population of these tables directly in a normalized way. What this means is that the TTP is persistent across ASIC architectures. As a result, the SDN application can scale across ASIC architectures without any modification. For example, a fixed pipeline for IP routing, policy routing or an MPLS flow could be made consistent across any ASIC implementation.

This document details how to use TTP with the RYU OpenFlow Controller.

RYU Controller Configuration

RYU controller comes with sample applications that enable user to jumpstart SDN deployment. These sample applications are stored in the following directory:

```
ls -l /home/sudhirmodali/ryu/ryu/app
total 292
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3647 Jul  5 00:12 bmpstation.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  1787 Jul  5 00:12 cbench.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali   817 Jul  5 00:12 conf_switch_key.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3903 Jul  5 00:12 example_switch_13.py
drwxrwxr-x 3 sudhirmodali sudhirmodali  4096 Jul  5 00:12 gui_topology
-rw-rw-r-- 1 sudhirmodali sudhirmodali     0 Jul  5 00:12 __init__.py
drwxrwxr-x 2 sudhirmodali sudhirmodali  4096 Jul  5 00:12 ofctl
-rw-rw-r-- 1 sudhirmodali sudhirmodali 26560 Jul  5 00:12 ofctl_rest.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  5943 Jul  5 00:12 rest_conf_switch.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali 38839 Jul  5 00:12 rest_firewall.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali 39625 Jul  5 00:12 rest_qos.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali 70869 Jul  5 00:12 rest_router.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3912 Jul  5 00:12 rest_topology.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3294 Jul  5 00:12 simple_switch_12.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  4742 Jul  5 00:12 simple_switch_13.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3485 Jul  5 00:18 simple_switch_13.pyc
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3916 Jul  5 00:12 simple_switch_14.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3889 Jul  5 00:12 simple_switch_igmp.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  4328 Jul  5 00:12 simple_switch_lacp.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3755 Jul  5 00:12 simple_switch.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  4954 Jul  5 00:12 simple_switch_snort.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  4979 Jul  5 00:12 simple_switch_stp.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  3792 Jul  5 00:12 simple_switch_websocket_13.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  9379 Jul  5 00:12 wsgi.py
-rw-rw-r-- 1 sudhirmodali sudhirmodali  4396 Jul  5 00:12 ws_topology.py
```

Among all the applications, "ofctl_rest.py" (highlighted above) enables openflow REST interface for an open flow capable switch. This program supports OpenFlow versions 1.0 through 1.5. This provides a good framework to develop the APIs for configuring open flow rules.

```
pica8@ubuntu:~$ pip install ryu
pica8@ubuntu:~$ cd ryu
pica8@ubuntu:~/ryu$ ryu-manager ryu.app.ofctl_rest --verbose

loading app ryu.app.ofctl_rest
loading app ryu.controller.ofp_handler
instantiating app None of DPSet
creating context dpset
creating context wsgi
instantiating app ryu.app.ofctl_rest of RestStatsApi
instantiating app ryu.controller.ofp_handler of OFPHandler
(24694) wsgi starting up on http://0.0.0.0:8080
connected socket:<eventlet.greenio.base.GreenSocket object at 0x7fc8a6756950> address:('172.16.0.112', 39589)
hello ev <ryu.controller.ofp_event.EventOFPHello object at 0x7fc8a6623350>
move onto config mode
EVENT ofp_event->dpset EventOFPSwitchFeatures
switch features ev version=0x5,msg_type=0x6,msg_len=0x20,xid=0xb0590b8d,OFPSwitchFeatures(auxiliary_id=0,capabilit
move onto main mode
EVENT ofp_event->dpset EventOFPStateChange
DPSET: register datapath <ryu.controller.controller.Datapath object at 0x7fc8a668ca10>
```

Another important tool required to work with APIs is one of the following:

1. POSTman : (https://www.getpostman.com)
2. Swagger : (http://swagger.io/swagger-ui/)

The following example will demonstrate the use of POSTman to configure the open flow rules. Typically, these tools are used with a single switch to determine the REST APIs required to configure the switch. POSTman has a facility to run the set of APIs in an iterative process to perform the task multiple times if required.

The following is the configuration on the switch required to configure TTP:

```
admin@PicOS-OVS$ovs-vsctl show-running-config

Open_vSwitch ab7af11d-fc7a-4e9c-8165-36e67f92d043
  Bridge "br0"
    Controller fb5f8fd6-aca8-49f9-add0-800cd6c4d840
      is_connected: true
      role: other
      status: {current_version="OpenFlow14", sec_since_connect="691372", state=ACTIVE}
      target: "tcp:172.16.0.123:6633"
    datapath_id: "5e3e00e09500169a"
    datapath_type: "pica8"
    Port "te-1/1/1"
      Interface "te-1/1/1"
        type: "pica8"
      tag: 1
      vlan_mode: trunk
    Port "br0"
      Interface "br0"
        mtu: 1500
        type: internal
    Port "te-1/1/2"
      Interface "te-1/1/2"
        type: "pica8"
      tag: 1
      vlan_mode: trunk
    protocols: ["OpenFlow14"]

  Pica8 6d736702-1adb-44f8-93e6-998166ca813f
    hardware_type: "5401"
    pica_ttp_enable: true
    pica_ttp_name: RouterTTP.json
```

Step 1: Setting the following environment variables in Postman helps in managing the variables

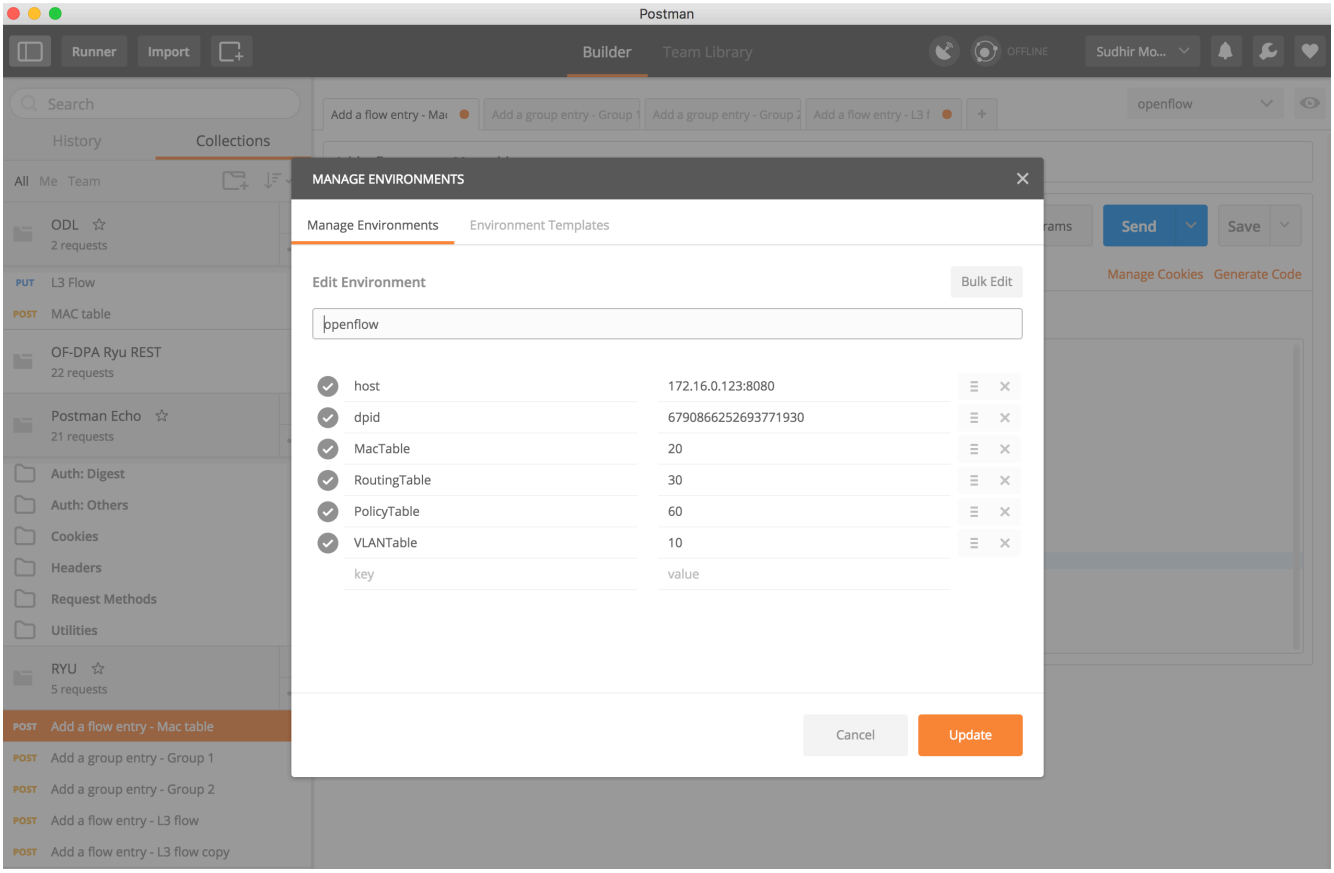
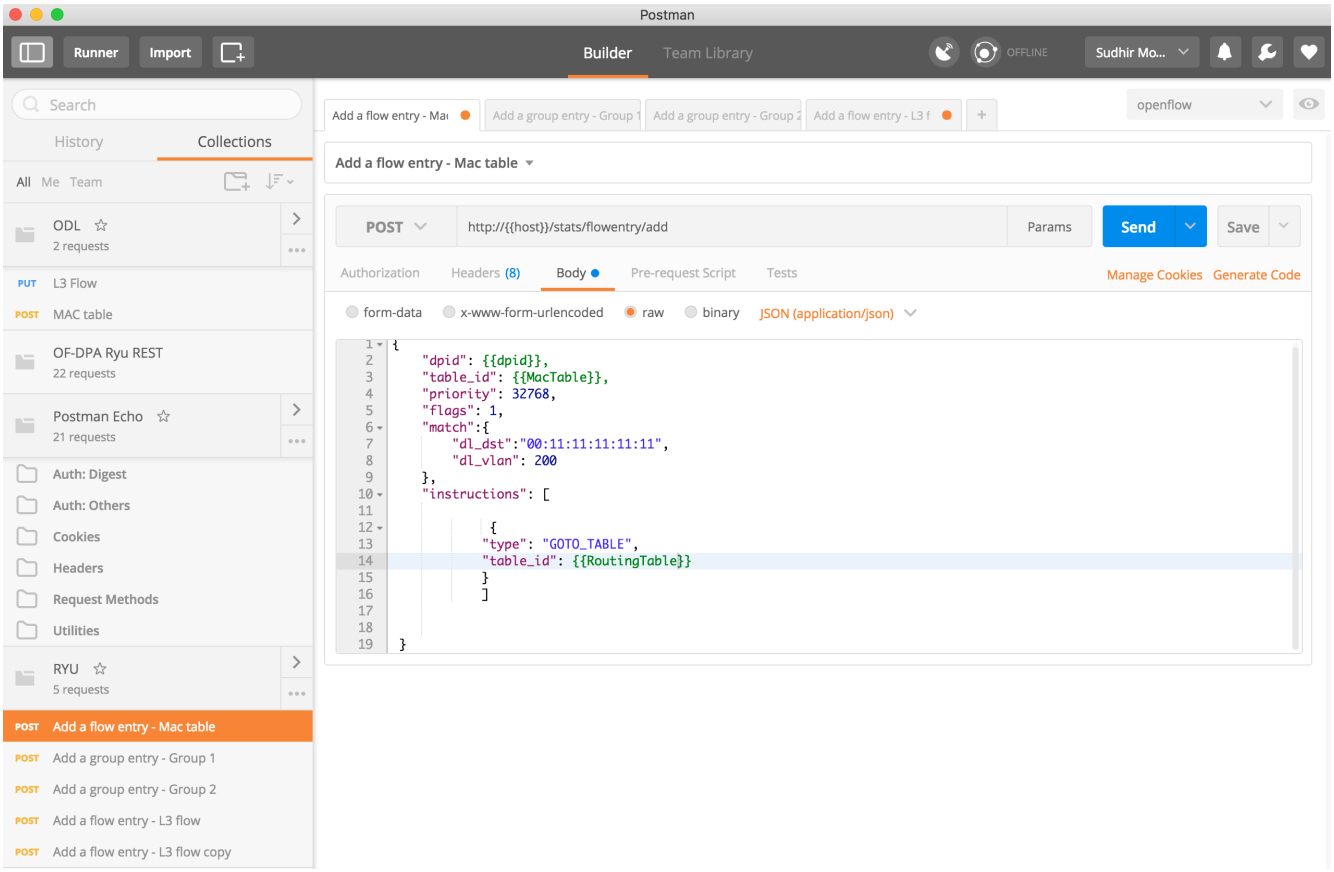


Table Type Patterns (TTP) are described in detail in the following blog (http://www.pica8.com/pica8-deep-dive/scaling-up-sdns-using-ttps-table-type-patterns/). The following is based on steps mentioned in the blog.

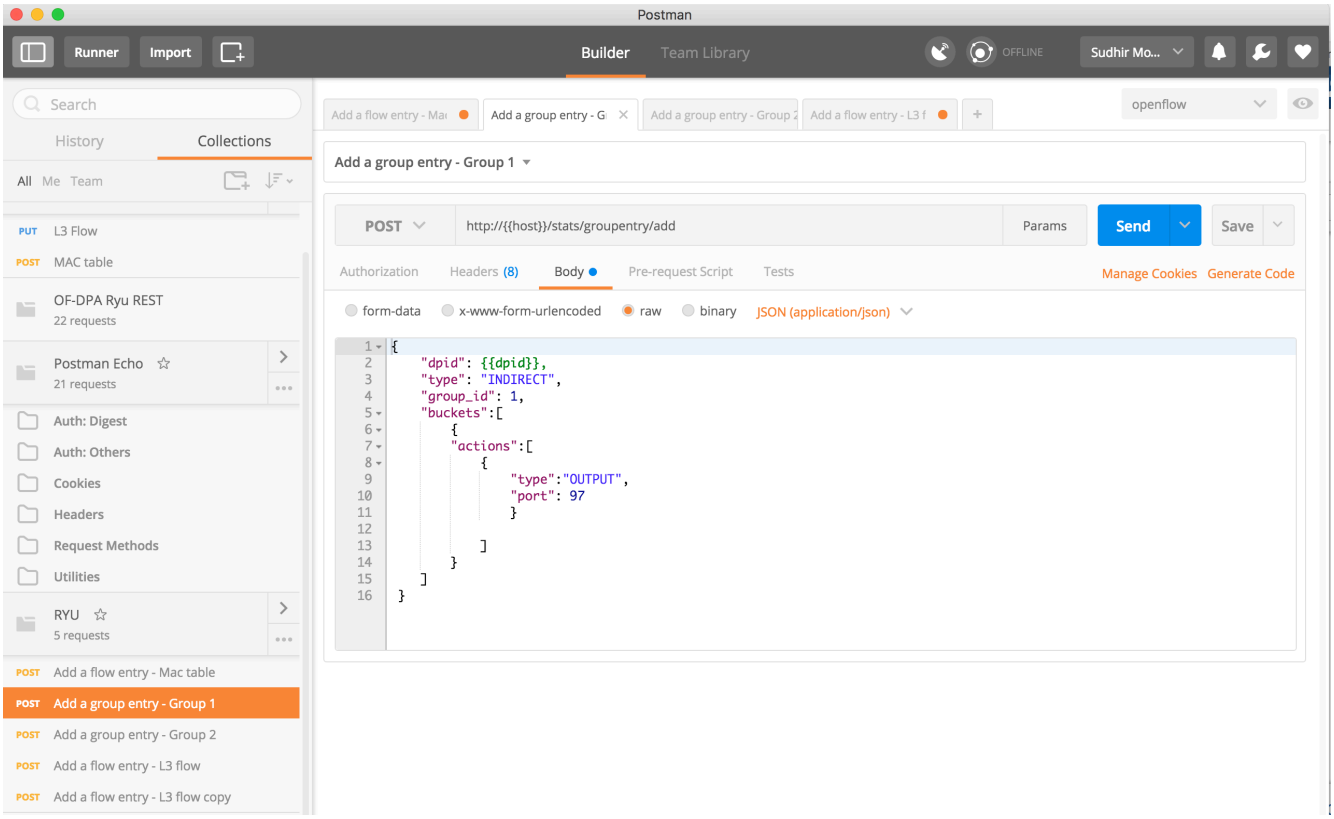
Step 2 : Creating a mac entry in the L2 table



Verify the switch has the flow configured

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0

OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=3735291, cookie=0x0, duration=690201.683s, table=20, n_packets=n/a, n_bytes=n/a, dl_vlan=200,dl_dst=00:11
```

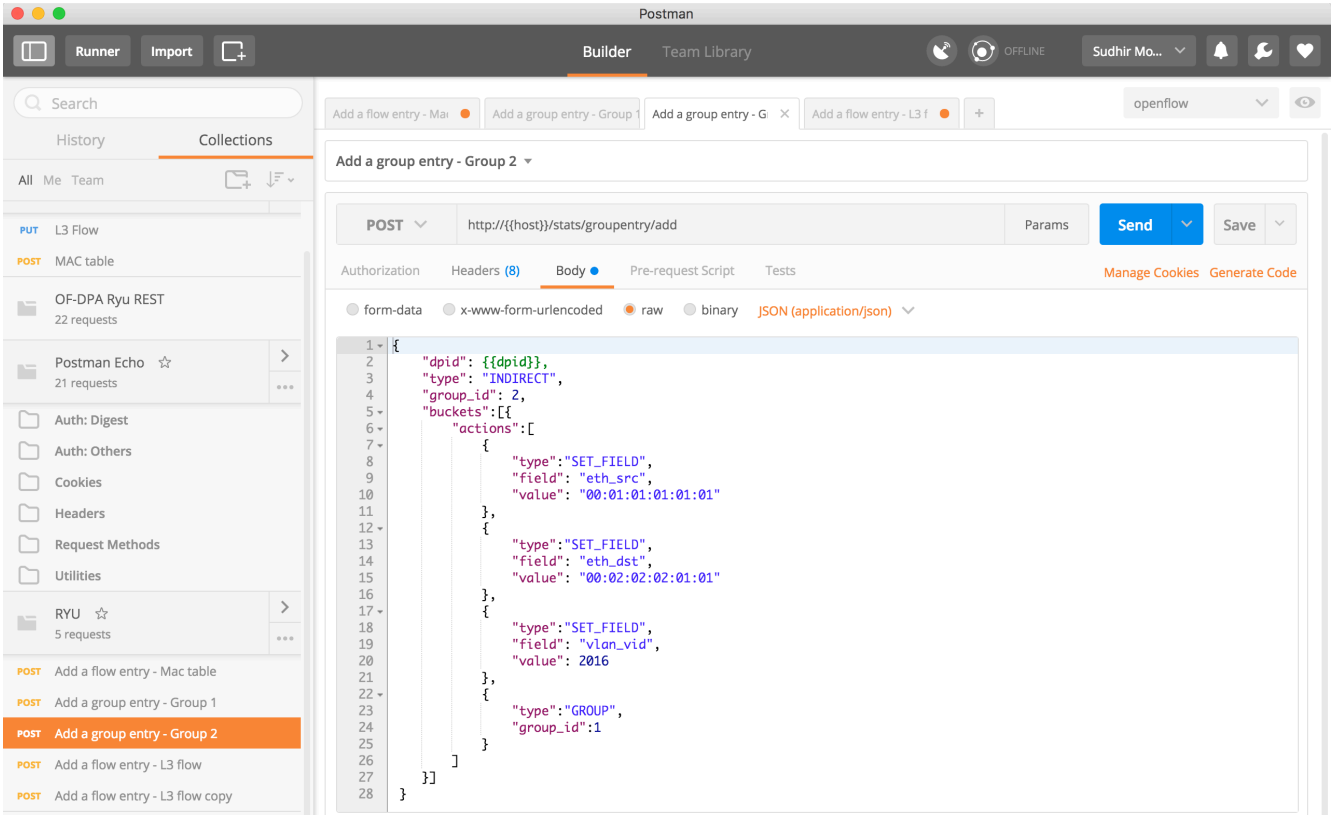
Step 3 : Creating a group entry (group_id = 1) for the egress L2 interface



Verify the group exists on the switch

```
admin@PicOS-OVS$ovs-ofctl dump-groups br0

OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
 group_id=1,type=indirect,bucket=weight:0,actions=output:97
```

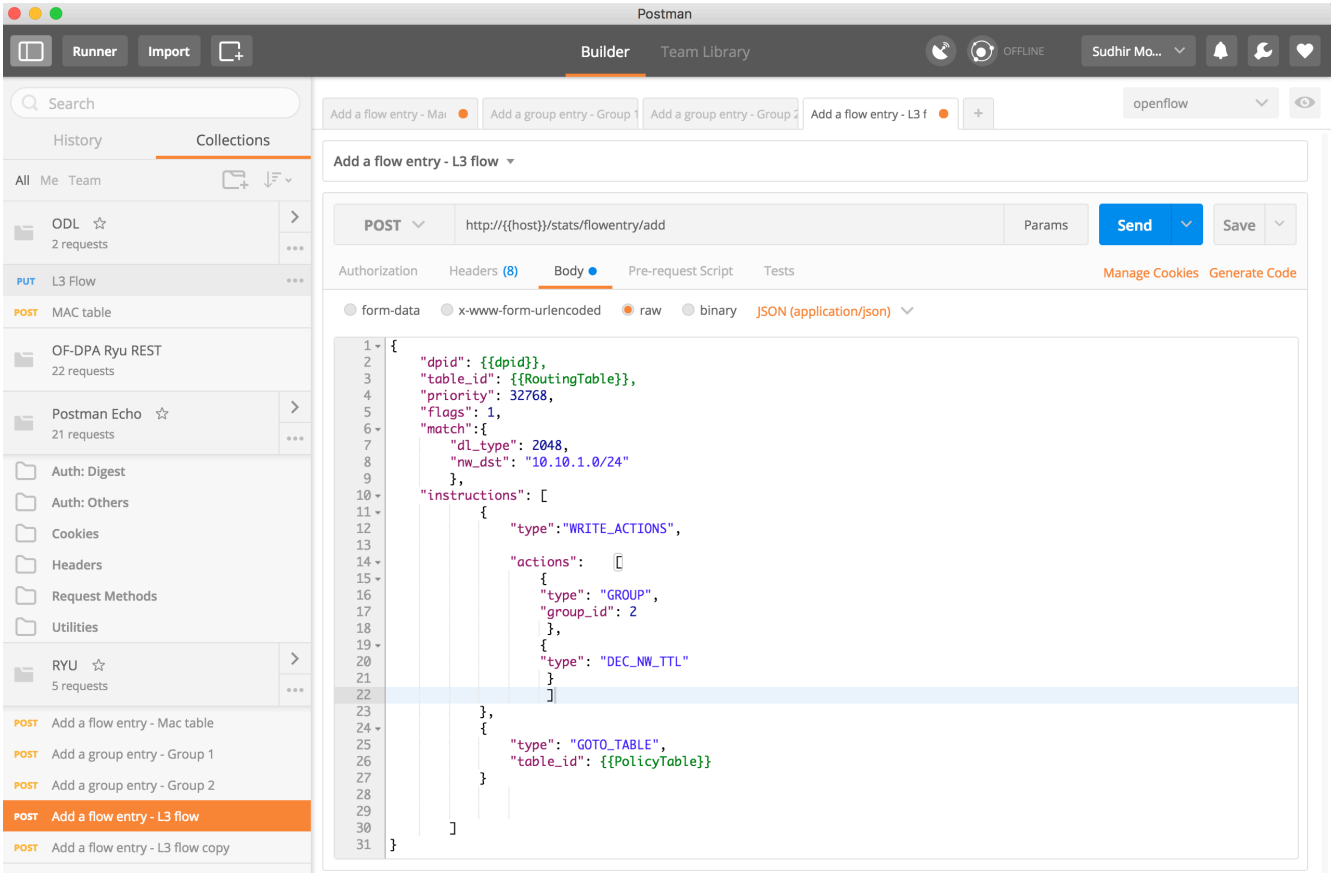
Step 4 : Create a group entry (group_id = 2) for the egress L3 interface



Verify the switch has the configuration

```
admin@PicOS-OVS$ovs-ofctl dump-groups br0

OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
 group_id=1,type=indirect,bucket=weight:0,actions=output:97
 group_id=2,type=indirect,bucket=weight:0,actions=set_field:00:01:01:01:01:01->eth_src,set_field:00:02:02:02:01:01
```

Step 5 : Create a IP flow in the L3 table



Verify the configuration on the switch

```
admin@PicOS-OVS$ovs-ofctl dump-flows br0

OFPST_FLOW reply (OF1.4) (xid=0x2):
 flow_id=3735291, cookie=0x0, duration=690201.683s, table=20, n_packets=n/a, n_bytes=n/a, dl_vlan=200,dl_dst=00:11
 flow_id=3735292, cookie=0x0, duration=690201.538s, table=30, n_packets=n/a, n_bytes=n/a, ip,nw_dst=10.0.1.0/24 act
```

"ovs-ofctl dump-flows br0" shows the software flow table configured by the controller. "ovs-appctl pica/dump-flows" shows the ASIC tables.

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows

Ingress Port Table: (Total 0 flows)

VLAN Table: (Total 0 flows)

Termination MAC Table: (Total 1 flows)
 ID=5 dl_vlan=200,dl_dst=00:11:11:11:11:11, actions:goto(Unicast Routing Table)

Unicast Routing Table: (Total 1 flows)
 ID=6 ip,nw_dst=10.0.1.0/24, actions:group(id=2,indirect,n=1,b0(set(dl_src=00:01:01:01:01:01,dl_dst=00:02:02:02:01

Policy ACL Table: (Total 1 flows)
 ID=1 priority=18000009,tcp,dl_dst=00:e0:95:00:16:9a,nw_src=172.16.0.123,tp_src=6633, actions:set(queue=7),output:(
```

Connection to OpenDaylight Controller

OpenDaylight is an open source platform for building programmable SDNs (software-defined networks). Learn more about OpenDaylight here.

- OpenDaylight Introduction
- Introduction to the OpenDaylight OpenFlow Controller
- Configure OVS for OpenDaylight Open Flow Controller
- OpenDaylight Controller-OVS Interaction
- OpenDaylight Simple Switch Application
- Message Type of Open Flow
- OVS Commands Reference 04

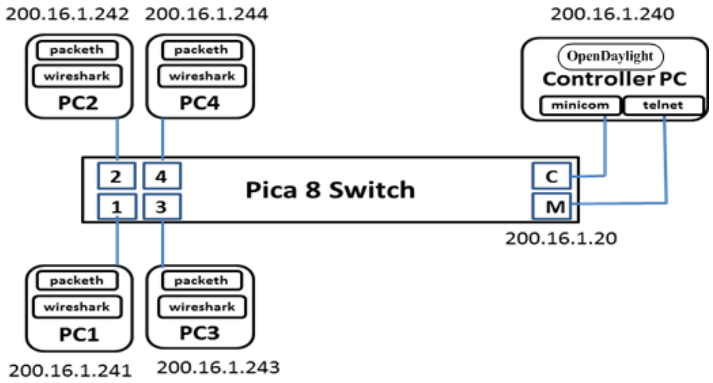
OpenDaylight Introduction

This document provides instructions on how to configure Pica8's open switches to work in various application scenarios. This guide assumes the reader has minimal to no knowledge of the Open Virtual Switch (OVS) implementation defined by http://openvswitch.org/; or the OpenFlow protocol, defined by https://www.opennetworking.org/. This guide will provide the tools required to configure Pica8's open switches as an OpenFlow switch. By reading this guide, user will gain insights on how to optimize the configuration to work in a specific application environment, while also learning about OVS and the OpenFlow protocol.

This starter kit provides screen shots and a list of off-the-shelf applications needed to complete the configuration, as well as tips on problems users may encounter during the setup. More documents or cookbooks on other subjects will be published periodically. This document provides a tutorial on how to:

- Configure Pica8 as an OVS OpenFlow switch
- Create bridges, add ports, show bridge and port statistics, status, and utilize the OVS database
- Configure flow tables for uni-directional, bi-directional, traffic switching, one-to-many multi-casting, mirroring, filtering, many-to-one aggregation, etc.
- Configure Pica8 OVS OpenFlow switches to interface with the OpenDaylight OpenFlow Controller

Figure 1 – Test bed configuration



In this document, the system configuration depicted in Figure 1 includes:

- A Pica8 P-3295 open switch with 48 x 1 GbE and 4 x 10 GbE uplinks
- 5 Linux PCs running Ubuntu 12.4.1 LTS, one is connected to the management LAN port (RJ45) and console port (RJ45F); this PC is referred to the controller PC. The OpenFlow controller will be running on this PC. Four PCs are connected to 1GbE port 1 to 4 and serve as a data terminal for generating and monitoring traffic
- Tools from installed on all the PCs are listed below. They can be installed through Linux installation utility *apt-get*
  - Terminal emulator minicom
  - Traffic monitoring tool Wireshark
  - Packet generator Packeth
  - ftp and ftpd

Introduction to the OpenDaylight OpenFlow Controller

OpenDaylight is an OpenFlow controller that has been integrated with the Pica8 open switch with OVS 1.10 implementation and supports Open Flow v1.3. Additional OpenDaylight information can be found at the OpenDaylight website http://www.opendaylight.org. The purpose of Pica8 OpenDaylight integration is to provide an open source SDN platform that the SDN community can prototype, test, and develop for application in an open source environment, with an open flow switching platform for real traffic testing. With the configuration provided in this starter kit, user should be able to have real traffic running within a week to test out the application scenarios using OVS command. Both OVS and OpenDaylight are open source with Apache licenses that developers can access easily.

User can obtain a copy of OpenDaylight from http://www.opendaylight.org/software/downloads. To install OpenDaylight, follow the procedure in the OpenDaylight Getting Started Guide.

After installing OpenDaylight, user can first edit the configuration file in */opendaylight/configuration/config.ini* and then start the OpenDaylight controller by using the ***./run.sh*** command.

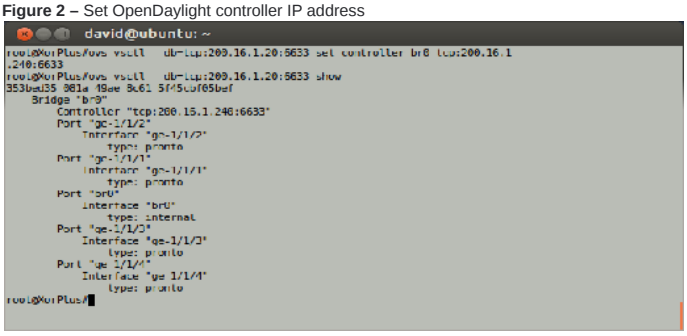
Figure 1

```
root@dev-42:/home/ychen/opendaylight# ./run.sh
osgi> 2014-05-27 10:45:50.871 CST [Start Level Event Dispatcher] INFO o.o.c.c.s.internal.ClusterManager - I'm a Gos
2014-05-27 10:45:51.016 CST [Start Level Event Dispatcher] INFO o.o.c.c.s.internal.ClusterManager - Started GossipR
GossipRouter started at Tue May 27 10:45:51 CST 2014
Listening on port 12001 bound on address 0.0.0.0/0.0.0.0
Backlog is 1000, linger timeout is 2000, and read timeout is 0
2014-05-27 10:45:51.016 CST [Start Level Event Dispatcher] INFO o.o.c.c.s.internal.ClusterManager - Starting the Cl
2014-05-27 10:45:52.075 CST [fileinstall-./plugins] INFO o.o.c.n.i.osgi.NetconfImplActivator - Starting TCP netconf
2014-05-27 10:45:52.341 CST [fileinstall-./plugins] INFO o.o.c.s.binding.impl.BrokerActivator - Binding Aware Broke
2014-05-27 10:45:52.556 CST [ConfigPersister-registrator] INFO o.o.c.n.p.i.ConfigPersisterNotificationHandler - Ses
2014-05-27 10:45:52.556 CST [ConfigPersister-registrator] INFO o.o.c.n.p.i.ConfigPersisterNotificationHandler - No
2014-05-27 10:45:55.705 CST [Start Level Event Dispatcher] INFO o.o.c.c.i.ConfigurationService - ConfigurationServi
2014-05-27 10:45:56.239 CST [ControllerI/O Thread] INFO o.o.c.p.o.core.internal.ControllerIO - Controller is now li
```

Configure OVS for OpenDaylight Open Flow Controller

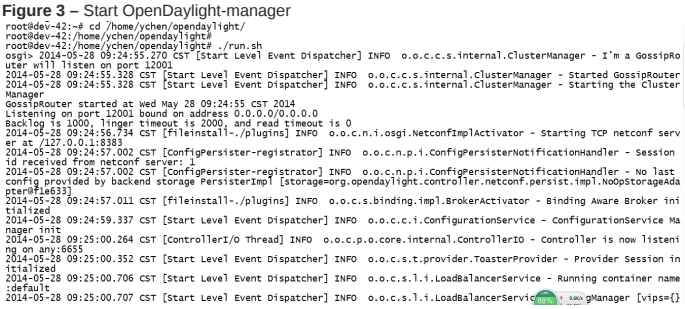
In OVS, the controller property of the bridge created earlier needs to be added to include the controller IP address and port number. The command ***ovs-vsctl set-controller br0 tcp:200.16.1.240:6633,*** is to set a controller address for bridge *br0.* The command ***ovs-vsctl show*** can now show the bridge information. The connection status is not shown because the controller has not been started yet.

Figure 2 – Set OpenDaylight controller IP address



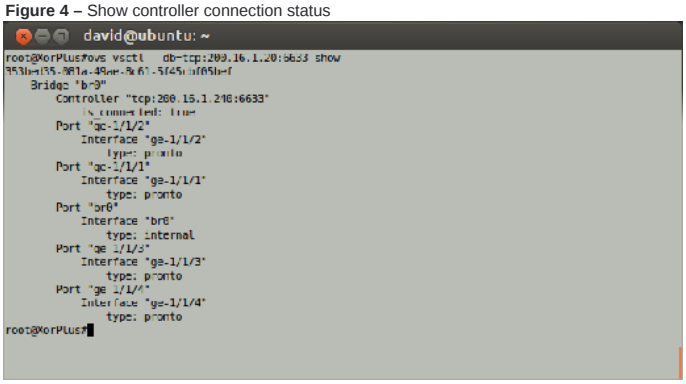
The OpenDaylight controller will be running on the controller PC with IP address 200.16.1.240, using default port 6633. The port number can be changed. For this exercise, the controller will be started with *"./run.sh"*

Figure 3 – Start OpenDaylight-manager



Once the controller is started, the connection status will change to *is_connected: true*. The controller port information can also be shown using the command ***ovs-ofctl show*** *br0*.

Figure 4 – Show controller connection status

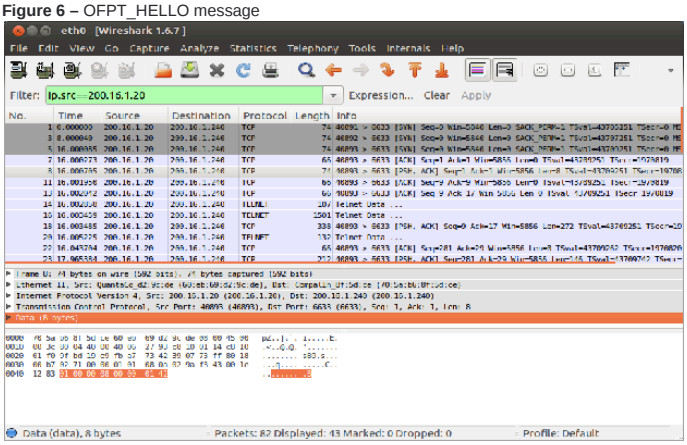


OpenDaylight Controller-OVS Interaction

Once the controller and OVS are connected, a set of messages will be exchanged. For example, the OVS sends an OFPT_HELLO message to the controller. The hello message is captured on the *wireshark* screen. The first byte of the message is the version number, and the second byte is the OFPT_TYPE. OFTP_HELLO message is type 0.

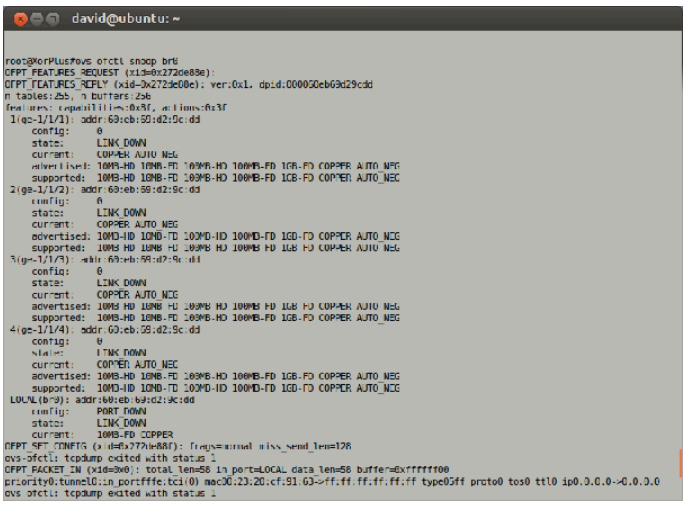
After the hello message from the switch, the controller sends OFPT_FEATURES_REQUEST (type=5) to retrieve the switch capabilities, including supported open flow version, switch configuration, and port hardware address. The switch sends OFPT_FEATURES_REPLY (type=6) to provide the feature information. The message is shown on both the controller console and the switch console.

Figure 6 – OFPT_HELLO message



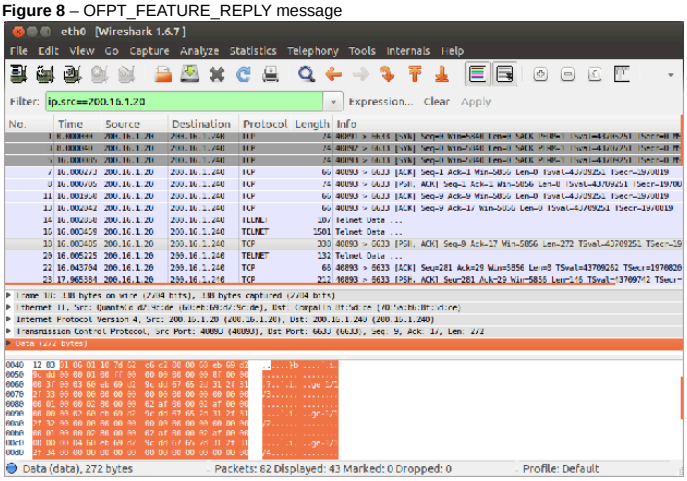
The switch console information is provided by the snoop option of the *ovs-ofctl* command. The command is ***ovs-ofctl snoop br0*.** It shows the feature request from the controller and the feature reply with the bridge information. User can compare the switch console information with the controller console information to get a better understanding of the message exchange.

Figure 7 – ovs-ofctl snoop br0



The *wireshark* also captured the information. Notice the message type in the second byte is 6 representing the OFPT_FEATURES_REPLY. After the feature reply, the controller sends an OFPT_SET_CONFIG message to set the message parameters like the max length, etc. Once the controller is connected, the OVS changes its default behavior from a layer 2 switch to an OVS switch. It means the flooding is disabled and open flow packet processing starts. Each packet is processed based on the flow table entry. Unmatched packet is forwarded to the controller for analysis unless a rule is defined to drop the packet. During initial start up with the controller, the flow table is empty. Therefore, packets received from any port are forwarded to the controller. The next message from the switch is type OFPT_PACKET_IN (type=10/0x0a).

Figure 8 – OFPT_FEATURE_REPLY message

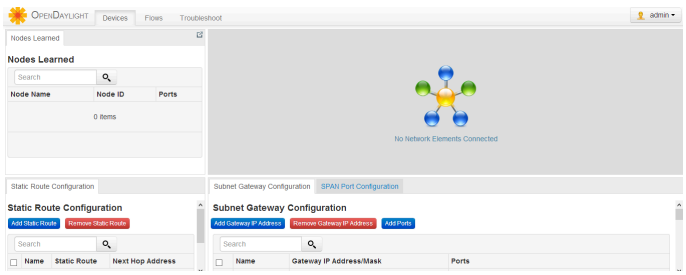


In this exercise, the *OpenDaylight controller* does not have any application to receive and process the OFPT_PACKET_IN message. Therefore, on the controller screen, a bunch of *unhandled_events* are printed on the console. At this point, the OpenDaylight-OVS open flow session is established and ready for Open Flow application to take over the event handling and flow configuration.

OpenDaylight Simple Switch Application

With only the controller connected, without any application, the ping between the PCs cannot work because the ARP requests are forwarded to the controller without any packet processing instructions in the flow tables. OpenDaylight code distribution comes with a set of applications to show how applications can be integrated. Next, an example will be shown of running the simple switch application. The application processes the *packet_in* messages (e.g., ICMP_REQUEST) and instructs the bridge to flood all other ports with the packets. Once the destination host receives the request and replies with its MAC address, this simple switch application sets up the flow table to forward traffic from source port to the correct destination port. This is the default switch behavior that has been tested. When starting the OpenDaylight controller with "/home/ychen/opendaylight# ./run.sh", user can configure the controller on the web, http://10.10.50.42:8080/

Figure 9 – Web configure



Message Type of Open Flow

```
# enum ofp_type
OFPT_HELLO = 0 # Symmetric message
OFPT_ERROR = 1 # Symmetric message
OFPT_ECHO_REQUEST = 2 # Symmetric message
OFPT_ECHO_REPLY = 3 # Symmetric message
OFPT_VENDOR = 4 # Symmetric message
OFPT_FEATURES_REQUEST = 5 # Controller/switch message
OFPT_FEATURES_REPLY = 6 # Controller/switch message
OFPT_GET_CONFIG_REQUEST = 7 # Controller/switch message
OFPT_GET_CONFIG_REPLY = 8 # Controller/switch message
OFPT_SET_CONFIG = 9 # Controller/switch message
OFPT_PACKET_IN = 10 # Async message
OFPT_FLOW_REMOVED = 11 # Async message
OFPT_PORT_STATUS = 12 # Async message
OFPT_PACKET_OUT = 13 # Controller/switch message
OFPT_FLOW_MOD = 14 # Controller/switch message
OFPT_PORT_MOD = 15 # Controller/switch message
OFPT_STATS_REQUEST = 16 # Controller/switch message
OFPT_STATS_REPLY = 17 # Controller/switch message
OFPT_BARRIER_REQUEST = 18 # Controller/switch message
OFPT_BARRIER_REPLY = 19 # Controller/switch message
OFPT_QUEUE_GET_CONFIG_REQUEST = 20 # Controller/switch message
OFPT_QUEUE_GET_CONFIG_REPLY = 21 # Controller/switch message
```

OVS Commands Reference 04

```
ovs-vsctl show
ovs-ofctl show br0
ovs-ofctl dump-ports br0
ovs-vsctl list-br
ovs-vsctl list-ports br0
ovs-vsctl list-ifaces br0
ovs-ofctl dump-flows br0
ovs-ofctl snoop br0
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl del-br br0
ovs-vsctl set-controller br0 tcp:172.16.1.240:6633
ovs-vsctl del-controller br0
ovs-vsctl set Bridge br0 stp_enable=true
ovs-vsctl add-port br0 ge-1/1/1 - set interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 - set interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 - set interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 - set interface ge-1/1/4 type=pica8
ovs-vsctl add-port br0 ge-1/1/1 type=pronto options:link_speed=1G
ovs-vsctl del-port br0 ge-1/1/1
ovs-ofctl add-flow br0 in_port=1,actions=output:2
ovs-ofctl mod-flows br0 in_port=1,dl_type=0x0800,nw_src=100.10.0.1,actions=output:2
ovs-ofctl add-flow br0 in_port=1,actions=output:2,3,4
ovs-ofctl add-flow br0 in_port=1,actions=output:4
ovs-ofctl del-flows br0
ovs-ofctl mod-port br0 1 no-flood
ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=192.168.1.241,actions=output:3
ovs-ofctl add-flow br0 in_port=4,dl_type=0x0800,dl_src=60:eb:69:d2:9c:dd,nw_src=198.168.1.2,nw_dst=124.12.123.55,actions=output:1
ovs-ofctl mod-flows br0 in_port=4,dl_type=0x0800,nw_src=192.210.23.45,actions=output:3
ovs-ofctl del-flows br0 in_port=1
```

Connection to a Floodlight Controller

- Floodlight Controller Introduction
- Floodlight Open Flow Controller
- Test Topology
- Configure OVS
- Launch Floodlight
- Floodlight REST Interface

Floodlight Controller Introduction

This is the fourth document of the *Open SDN Starter Kit series*. This document provides instructions on how to configure Pica8's open switches in order to work with *Floodlight Controller*. This document assumes the reader has read the first two documents of the *Open SDN Starter Kit series*.

Floodlight Open Flow Controller

The *Floodlight* Open SDN Controller is an enterprise-class, Apache-licensed, Java-based OpenFlow Controller and it supports OpenFlow v1.0. In fact, *Floodlight* is not just an OpenFlow controller and it also includes a collection of applications built on top the *Floodlight* Controller. Additional *Floodlight* information can be found at *Floodlight* website http://www.projectfloodlight.org/floodlight/.

Users can either download the *Floodlight* source from http://www.projectfloodlight.org/download/ or follow the *Installation Guide,* http://docs.projectfloodlight.org/display/floodlightcontroller/Installation+Guide to install *Floodlight*.
In this document, we follow the *Installation Guide* to clone the source to an Ubuntu 11.10 system:

Figure 1 – Clone Floodlight

```
frank@ubuntu:~/wd/pica8/bigswitch/test$ git clone git://github.com/floodlight/floodlight.git
Cloning into floodlight...
remote: Counting objects: 24067, done.
remote: Compressing objects: 100% (9042/9042), done.
remote: Total 24067 (delta 12504), reused 23511 (delta 11994)
Receiving objects: 100% (24067/24067), 26.64 MiB | 960 KiB/s, done.
Resolving deltas: 100% (12504/12504), done.
frank@ubuntu:~/wd/pica8/bigswitch/test$ ls
floodlight
frank@ubuntu:~/wd/pica8/bigswitch/test$ cd floodlight/
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$ git checkout fl-last-passed-build
Note: checking out 'fl-last-passed-build'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

  git checkout -b new_branch_name

HEAD is now at e890662... Merge pull request #405 from vy/patch-5
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$
```

Why Make Changes?

By default, *Floodlight* forwards the unknown packets from the Pica8 switch to the destination. In this case, things may go well even if there are no flows set in the Pica8 switch. The purpose of this document is to show users how to use Floodlight REST interface to add flows to the Pica8 switch and verify the transmission of the traffic. In order to eliminate the confusion whether the packets are forwarded by Pica8 switch or *Floodlight* controller, we will disable *Floodlight*'s default forwarding feature.

Changes to Floodlight

The *Floodlight*'s default setting is in $floodlight/src/resources/floodlightdefault.properties. We need to remove the line "net.floodlightcontroller.forwarding.Forwarding,\" as shown below:

Figure 2 – Edit Floodlight Default Properties

```
floodlight.modules = net.floodlightcontroller.storage.memory.MemoryStorageSource,\
net.floodlightcontroller.core.FloodlightProvider,\
net.floodlightcontroller.threadpool.ThreadPool,\
net.floodlightcontroller.devicemanager.internal.DeviceManagerImpl,\
net.floodlightcontroller.devicemanager.internal.DefaultEntityClassifier,\
net.floodlightcontroller.staticflowentry.StaticFlowEntryPusher,\
net.floodlightcontroller.firewall.Firewall,\
net.floodlightcontroller.forwarding.Forwarding,\
net.floodlightcontroller.linkdiscovery.internal.LinkDiscoveryManager, \
net.floodlightcontroller.topology.TopologyManager, \
net.floodlightcontroller.flowcache.FlowCache, \
net.floodlightcontroller.flowcache.FlowReconcileManager, \
net.floodlightcontroller.jython.JythonDebugInterface,\
net.floodlightcontroller.counter.CounterStore,\
net.floodlightcontroller.debugcounter.DebugCounter,\
net.floodlightcontroller.perfmon.PktInProcessingTime,\
net.floodlightcontroller.ui.web.StaticWebRoutable,\
net.floodlightcontroller.loadbalancer.LoadBalancer
net.floodlightcontroller.restserver.RestApiServer.port = 8080
net.floodlightcontroller.core.FloodlightProvider.openflowport = 6633
net.floodlightcontroller.jython.JythonDebugInterface.port = 6655
net.floodlightcontroller.forwarding.Forwarding.idletimeout = 5
net.floodlightcontroller.forwarding.Forwarding.hardtimeout = 0
```

Build Floodlight

Before building *Floodlight*, we need to install *JDK* and *Ant*. Then, issue *ant* to build *Floodlight*.

Figure 3 – Build Floodlight

```
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$ ant
Buildfile: /home/frank/wd/pica8/bigswitch/test/floodlight/build.xml

init:
    [mkdir] Created dir: /home/frank/wd/pica8/bigswitch/test/floodlight/target/bin
    [mkdir] Created dir: /home/frank/wd/pica8/bigswitch/test/floodlight/target/bin-test
    [mkdir] Created dir: /home/frank/wd/pica8/bigswitch/test/floodlight/target/lib
    [mkdir] Created dir: /home/frank/wd/pica8/bigswitch/test/floodlight/target/test

compile:
    [javac] Compiling 397 source files to /home/frank/wd/pica8/bigswitch/test/floodlight/target/bin
    [javac] Note: Some input files use unchecked or unsafe operations.
    [javac] Note: Recompile with -Xlint:unchecked for details.
     [copy] Copying 52 files to /home/frank/wd/pica8/bigswitch/test/floodlight/target/bin

compile-test:
    [javac] Compiling 79 source files to /home/frank/wd/pica8/bigswitch/test/floodlight/target/bin-test

dist:
      [jar] Building jar: /home/frank/wd/pica8/bigswitch/test/floodlight/target/floodlight.jar
      [jar] Building jar: /home/frank/wd/pica8/bigswitch/test/floodlight/target/floodlight-test.jar

BUILD SUCCESSFUL
Total time: 55 seconds
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$
```

Then, the *Floodlight* Java Archive file, *floodlight.jar*, is generated under *target* directory and ready to be run.

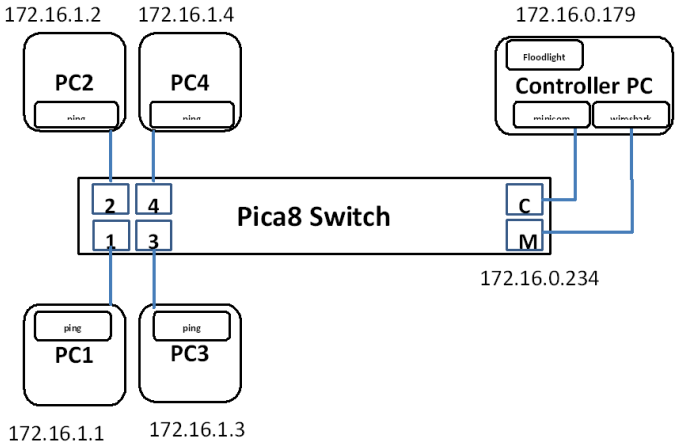
Figure 4 – floodlight.jar

```
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$ ls
apps                   floodlight_style_settings.xml  NOTICE.txt
build.xml              lib                            README.md
example                LICENSE.txt                    setup-eclipse.sh
findbugs-exclude.xml   logback.xml                    src
floodlight.sh          Makefile                       target
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$ ls target
bin  bin-test  floodlight.jar  floodlight-test.jar  lib  test
frank@ubuntu:~/wd/pica8/bigswitch/test/floodlight$
```

Test Topology

The following picture shows the test topology which is similar to the topology in the first two documents of the *Open SDN Starter Kit series,* even though the IP addresses are different.

Figure 5 – Test Topology



In this document, the systems depicted in the above diagram include:

- A Pica8 switch which is P-3295
- 5 Linux PCs running Ubuntu 11.10
  - The one, connected to the P-3295 management port (RJ45) and console port (RJ45F), is referred as the controller PC. The *Floodlight* controller will be running on this PC.
  - The other four PCs are connected to physical port 1 to 4 and serve as a data terminal to verify the flow.

Configure OVS

In this document, we start OVS manually. After powering on the Pica8 switch, users will see the following messages on the console display. Select choice "2" for OVS and enter "yes" to start OVS by manual.

Figure 6 – Start OVS Manually

```
Flash Information :
  Device Id         : 0x00000022
  Device Flags      : 0x00000000
  Device Blocks     : 0x00000100
  Device Block Info : 0x00020000

I2C Device Drivers (c) 2007 Quanta Computer Inc.
Registered with major 242

PCI Driver v0.10 (c) 2007 Quanta Computer Inc.
Registered with major 244

WDT Driver v0.1 (c) 2008 Quanta Computer Inc.
Registered with major 245
linux_kernel_bde: module license 'Proprietary' taints kernel.
Checking file system integrity on '/dev/hda1' ...

File system OK
net.netfilter.nf_conntrack_acct = 1
net.ipv6.conf.all.forwarding = 1
System initiating...Please wait...
    Please choose which to start: PicOS L2/L3, PicOS OVS/OpenFlow, or System She
ll:
        (Will choose default entry if no input in 10 seconds.)
        [1]  PicOS L2/L3    * default
        [2]  PicOS Open vSwitch/OpenFlow
        [3]  System Shell
        [4]  Boot Menu Editor
Enter your choice (1,2,3,4):2

PicOS Open vSwitch/OpenFlow is selected.

  Note: Defaultly, the OVS server is runned with static local management IP and
port 6633.
        The default way of vswitch connecting to server is PTCP.
        If you do not want default configuration, choose manual start!

sh: you need to specify whom to kill
Do you want start the OVS by manual? (yes/no) yes
You need start troot@PicOS-OVS#
root@PicOS-OVS#
```

Please refer to PicOS 1.6 OVS Configuration Guide, http://www.pica8.org/document/picos-1.6-ovs-configuration-guide.pdf, for the details how to configure OVS. First, we need to provide a fixed IP address to the Pica8 switch, create the OVS database, and launch the OVS database server and the switch daemon. Here are the commands:

- ifconfig eth0 172.16.0.234/24
- ovsdb-tool create /ovs/ovs-vswitchd.conf.db /ovs/bin/vswitch.ovsschema
- ovsdb-server /ovs/ovs-vswitchd.conf.db --remote=ptcp:6632:172.16.0.234 &
- ovs-vswitchd tcp:172.16.0.234:6632 --pidfile=pica8 --overwrite-pidfile > /var/log/ovs.log 2> /dev/null &

Figure 7 – Configure OVS - 1

```
root@PicOS-OVS#ifconfig eth0 172.16.0.234/24
root@PicOS-OVS#PHY: 24520:00 - Link is Up - 1000/Full
ovsdb-tool create /ovs/ovs-vswitchd.conf.db /ovs/bin/vswitch.ovss
chema
root@PicOS-OVS#
root@PicOS-OVS#ovsdb-server /ovs/ovs-vswitchd.conf.db --remote=ptcp:6632:172.16.
0.234 &
root@PicOS-OVS#2013-06-11T19:17:50Z|00001|ovsdb_server|INFO|ovsdb-server (Open v
Switch) 1.9.90

root@PicOS-OVS#ovs-vswitchd tcp:172.16.0.234:6632 --pidfile=pica8 --overwrite-pi
dfile > /var/log/ovs.log 2> /dev/null &
```

In the following steps, we create the bridge, br0, and add 4 physical ports to it and set up its connection to a specific OpenFlow Controller (*Floodlight* in this case):

- ovs-vsctl add-br br0 – set bridge br0 datapath_type=pica8
- ovs-vsctl add-port br0 ge-1/1/1 – set interface ge-1/1/1 type=pica8
- ovs-vsctl add-port br0 ge-1/1/2 – set interface ge-1/1/2 type=pica8
- ovs-vsctl add-port br0 ge-1/1/3 – set interface ge-1/1/3 type=pica8
- ovs-vsctl add-port br0 ge-1/1/4 – set interface ge-1/1/4 type=pica8
- ovs-vsctl set-controller br0 tcp:172.16.0.179:6633

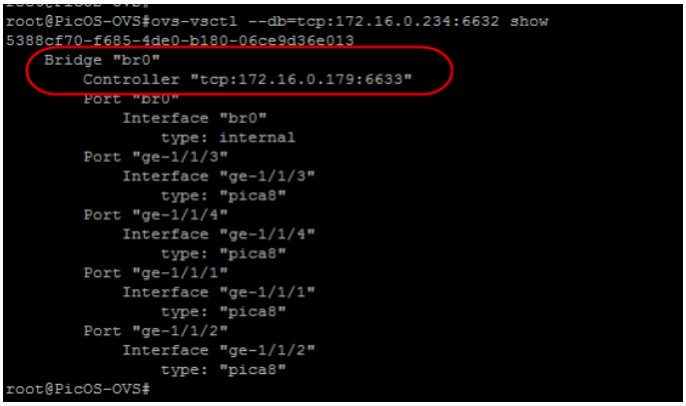
Figure 8 – Configure OVS - 2

```
root@PicOS-OVS#
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 add-br br0  -- set bridge br
0 datapath_type=pica8
device ovs-pica8 entered promiscuous mode
device br0 entered promiscuous mode
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 add-port br0 ge-1/1/1 -- set
 interface ge-1/1/1 type=pica8
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 add-port br0 ge-1/1/2 -- set
 interface ge-1/1/2 type=pica8
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 add-port br0 ge-1/1/3 -- set
 interface ge-1/1/3 type=pica8
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 add-port br0 ge-1/1/4 -- set
 interface ge-1/1/4 type=pica8
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 set-controller br0 tcp:172.1
6.0.179:6633
root@PicOS-OVS#
```

We can verify the configuration by issuing:

- ovs-vsctl show

Figure 9 – Show OVS Configuration

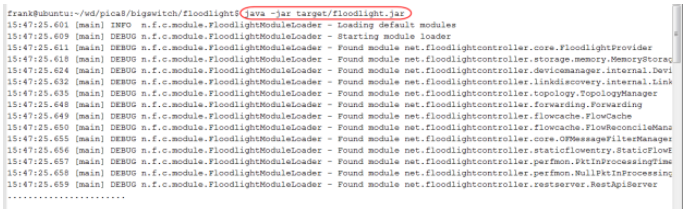


In the above pictures, it shows that the OpenFlow Controller has been defined. After the connection between Pica8 switch and OpenFlow Controller, the same command will show the connection status.

Launch Floodlight

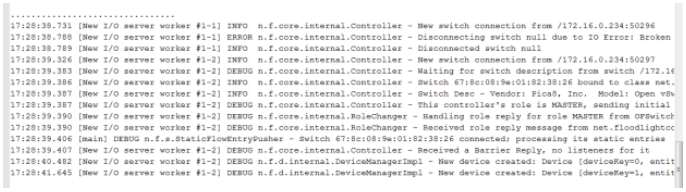
It makes no difference whether to launch *Floodlight* before or after bringing up Pica8 switch. In this document, we start *Floodlight* after bringing up Pica8 switch.

Figure 10 – Start Floodlight



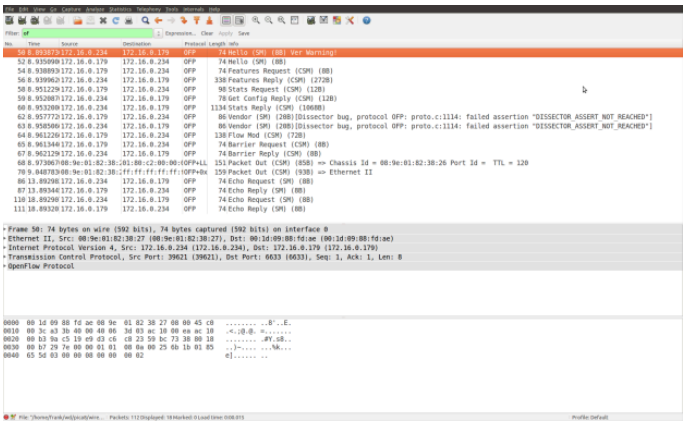
The following figure shows the connection between Pica8 switch and *Floodlight*.

Figure 11 – Start Floodlight



We can also use Wireshark to capture the traffic between Pica8 switch and Floodlight as shown below:

Figure 12 – Wireshark Captures



We can also use the following command to show the connection status:

- ovs-vsctl show

Figure 13 – Show OVS Connection Status

```
root@PicOS-OVS#ovs-vsctl --db=tcp:172.16.0.234:6632 show
5388cf70-f685-4de0-b180-06ce9d36e013
    Bridge "br0"
        Controller "tcp:172.16.0.179:6633"
            is_connected: true
        Port "br0"
            Interface "br0"
                type: internal
        Port "ge-1/1/3"
            Interface "ge-1/1/3"
                type: "pica8"
        Port "ge-1/1/4"
            Interface "ge-1/1/4"
                type: "pica8"
        Port "ge-1/1/1"
            Interface "ge-1/1/1"
                type: "pica8"
        Port "ge-1/1/2"
            Interface "ge-1/1/2"
                type: "pica8"
root@PicOS-OVS#
root@PicOS-OVS#
```

We can now use the following command to verify that all of the physical ports are connected:

- ovs-ofctl show br0

Figure 14 – Show Physical Port Status

```
root@PicOS-OVS#ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.2) (xid=0x2): dpid:678c089e01823826
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS
 1(ge-1/1/1): addr:08:9e:01:82:38:26
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER AUTO_NEG
     advertised: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     peer:       10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER
     speed: 1000 Mbps now, 1000 Mbps max
 2(ge-1/1/2): addr:08:9e:01:82:38:26
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER AUTO_NEG
     advertised: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     peer:       10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER
     speed: 1000 Mbps now, 1000 Mbps max
 3(ge-1/1/3): addr:08:9e:01:82:38:26
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER AUTO_NEG
     advertised: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     peer:       10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER
     speed: 1000 Mbps now, 1000 Mbps max
 4(ge-1/1/4): addr:08:9e:01:82:38:26
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER AUTO_NEG
     advertised: 10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     supported:  10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER AUTO_NEG
     peer:       10MB-HD 10MB-FD 100MB-HD 100MB-FD 1GB-FD COPPER
     speed: 1000 Mbps now, 1000 Mbps max
 LOCAL(br0): addr:08:9e:01:82:38:26
     config:     0
     state:      LINK_UP
     current:    10MB-FD COPPER
     supported:  10MB-FD COPPER
     speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.2) (xid=0x4): frags=normal miss_send_len=0
root@PicOS-OVS#
```

At this moment, there are no flows defined:

- ovs-ofctl dump-flows br0

Figure 15 – No Flows defined in Pica8 Switch

```
root@PicOS-OVS#
root@PicOS-OVS#ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.2) (xid=0x2):
root@PicOS-OVS#
```

If we try to ping from PC1 to PC2, it fails:

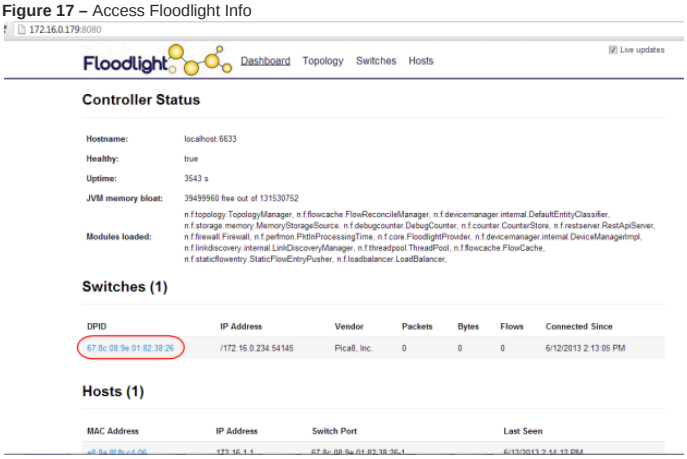
Figure 16 – Ping Fails

```
PC1> ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
From 172.16.1.1 icmp_seq=1 Destination Host Unreachable
From 172.16.1.1 icmp_seq=2 Destination Host Unreachable
From 172.16.1.1 icmp_seq=3 Destination Host Unreachable
From 172.16.1.1 icmp_seq=4 Destination Host Unreachable
From 172.16.1.1 icmp_seq=5 Destination Host Unreachable

--- 172.16.1.2 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4016ms pipe 3
```

Floodlight REST Interface

We can use the browser to view *Floodlight*'s real time information. The URL can be http://172.16.0.179:8080/ui/index.html or http://127.0.0.1:8080/ui/index.html if users access it from Controller PC.

Figure 17 – Access Floodlight Info



User should pay attention to the DPID in the picture above. User needs to replace it with user's own DPID in the following tests.

curl

Use the command line tool curl for transferring data with URL syntax. It is also the tool to send Floodlight REST APIs to configure Pica8 switch flows. We can use apt-get to install it on Controller PC:

- sudo apt-get install curl

Add Flows

Here is the command to add a flow from port 1 to port 2:

- curl -d '{"switch": "67:8c:08:9e:01:82:38:26", "name":"pc1-pc2", "cookie":"0", "priority":"0", "ingress-port":"1", "active":"true", "actions":"output=2"}' http://127.0.0.1:8080/wm/staticflowentrypusher/json

We need another flow from port 2 to port 1 in order to make the ping between PC1 and PC2 work.

- curl -d '{"switch": "67:8c:08:9e:01:82:38:26", "name":"pc2-pc1", "cookie":"0", "priority":"0", "ingress-port":"2", "active":"true", "actions":"output=1"}' http://127.0.0.1:8080/wm/staticflowentrypusher/json

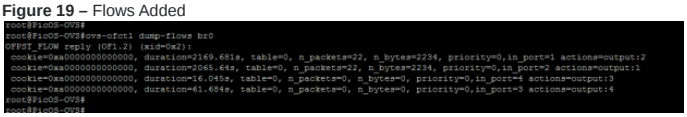
Now, the ping from PC1 to PC2 works.

Figure 18 – Ping Successes

```
PC1> ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_req=1 ttl=64 time=1.83 ms
64 bytes from 172.16.1.2: icmp_req=2 ttl=64 time=0.176 ms
64 bytes from 172.16.1.2: icmp_req=3 ttl=64 time=0.159 ms
64 bytes from 172.16.1.2: icmp_req=4 ttl=64 time=0.133 ms
64 bytes from 172.16.1.2: icmp_req=5 ttl=64 time=0.154 ms

--- 172.16.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.133/0.491/1.833/0.671 ms
PC1>
```

We can add the same flows between port 3 and port 4 to make ping working between them.

Figure 19 – Flows Added



Delete Flows

We can remove all of the flows by issuing:

- curl http://127.0.0.1:8080/wm/staticflowentrypusher/clear/67:8c:08:9e:01:82:38:26/json

Configuration Guide for Atrium Stack on ONOS Controller

ONOS is a production ready controller software, capable of enabling applications at scale with its architecture. To get more information on ONOS, please visit their home page.

ONF developed a BGP router application on the ONOS controller called the Atrium. This is a fully functional production ready peering application that uses OpenFlow enabled switches. To get relevant roadmap information and additional information on Atrium, please refer to the Atrium page.

- ONOS Introduction
- Installation Guide
- ONOS Configuration Guide
- Quagga Configuration Guide
- PicOS Configuration Guide
- How to Install ONOS

ONOS Introduction

ONOS

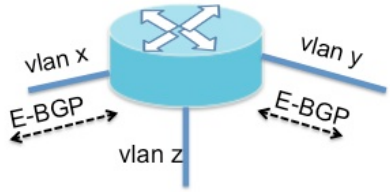
ONOS (Open Network Operating System) is the first open source SDN network operating system targeted specifically at the service provider and mission critical networks. ONOS is purpose built to provide high availability (HA), scale out, and performance for large scale networks. In addition, ONOS has useful Northbound abstractions and APIs to enable easier application development, as well as Southbound abstractions and interfaces to control OpenFlow ready and legacy devices. Thus, ONOS will:

- bring carrier grade features (scale, availability, and performance) to the SDN control plane
- enable web style agility
- help service providers migrate their existing networks to white boxes
- lower service provider CapEx and OpEx

ONOS has been developed in concert with leading service providers (AT&T, NTT Communications), R&E network operators (Internet2, CNIT, CREATE=NET), collaborators (SRI, Infoblox), and with ONF to validate its architecture through real world use cases.

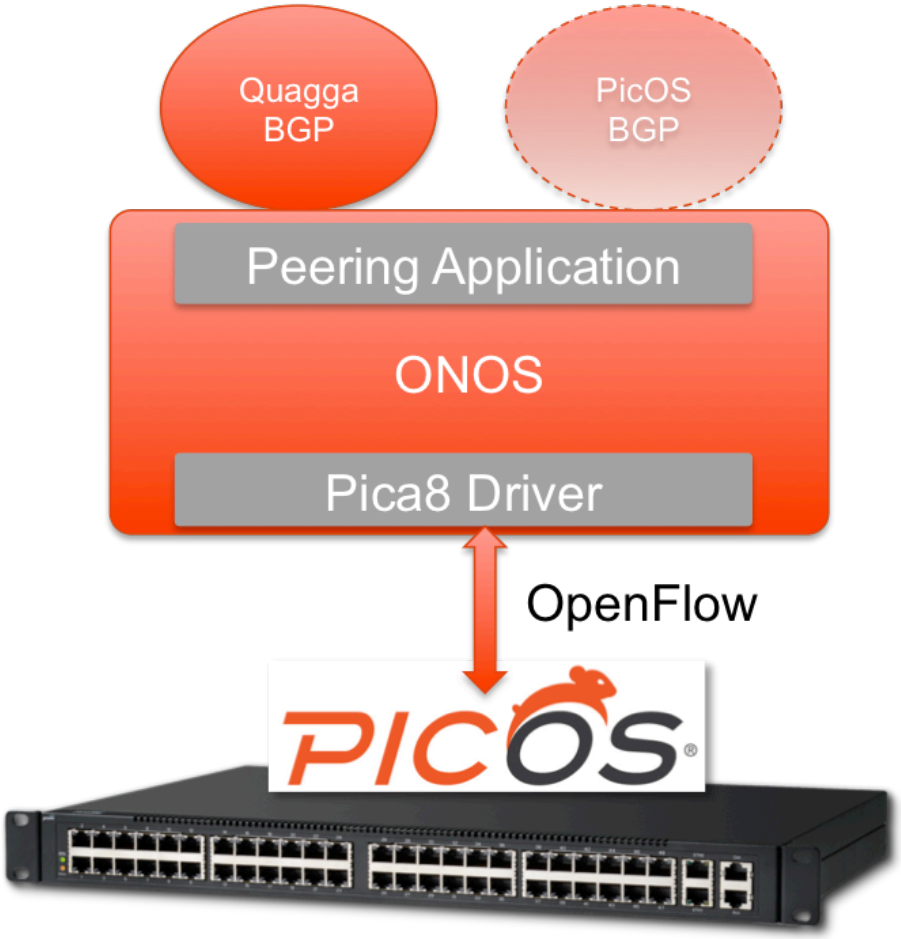
Atrium

In the first release (2015/A), Atrium is an open-source router that speaks BGP with other routers and programs flows on the open flow switch packets between ports or VLANs based on the next-hop learned via BGP peering.



Atrium creates a vertically-integrated stack to produce an SDN based router. This stack can have the forms shown below.

The stack includes a controller (ONOS) with a peering application (called BGP Router) integrated with an instance of Quagga BGP. The controller uses OpenFlow v1.3.4 to communicate with the hardware switch. The peering application uses multi-tables to install flows on the switch.


Quagga
BGP
PicOS
BGP
Peering Application
ONOS
Pica8 Driver
OpenFlow
PICOS

Installation Guide

Distribution VM

To get started with Atrium Release 2015/A, download the distribution VM (Atrium_2015_A.ova) from here: size ~ 2GB

https://www.dropbox.com/s/vw7k5y2vkhfytgx/Atrium_2015_A.ova?dl=0

login: admin

password: bgprouter

NOTE: This distribution VM is NOT meant for development. The only purpose is to help get a working system up and running for testing and deployment as painlessly as possible. A developer guide using mechanisms other than this VM will be available shortly after the release.

The VM can be run on any desktop, laptop, or server with virtualization software (VirtualBox, Parallels, VMWare Fusion, VMWare Player, etc.). We recommend using VirtualBox for non-server uses. For running on a server, see the subsection below.

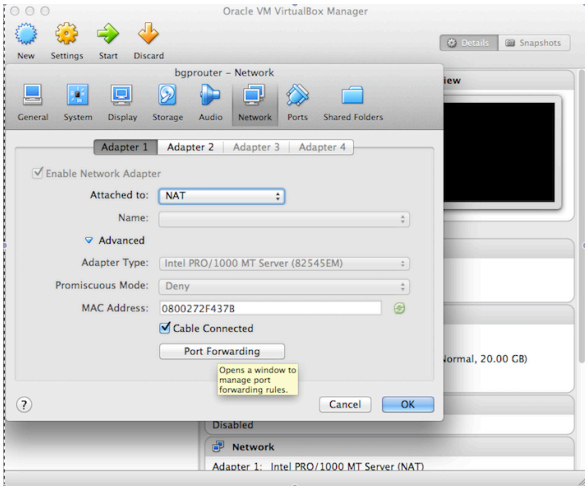
Get a recent version of VirtualBox to import and run the VM. We recommend the following:

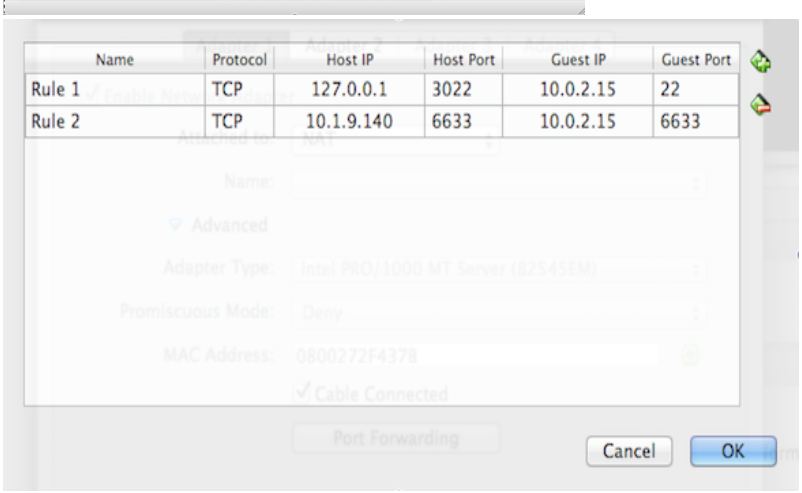
1) using 2 cores and at least 4GB of RAM.

2) For networking, user can "Disable" the **2nd** Network Adapter. We only need the 1st network adapter for this release.

3) User could choose the primary networking interface (Adapter 1) for the VM to be NATed or "bridged". If choosing to NAT, user would need to create the following port-forwarding rules. The first rule allows user to ssh into user's VM with a command from a Linux or MAC terminal like the one below:

```
$ ssh -X -p 3022 admin@localhost
```





The second rule allows user to connect an external switch to the controller running within the VM (the guest-machine) using the IP address of the host-machine (in the example its 10.1.9.140) on the host-port 6633.

If choosing to bridge (with DHCP) instead of NAT, user should login to the VM to see what IP address was assigned by user's DHCP server (on the eth0 interface). Then, user should use ssh to get in to the VM from a terminal:

```
$ ssh -X admin@<assigned-ip-addr>
```

User can login to the VM with the following credentials --> **login:** admin, **password:** bgprouter

Once in, user should try to ping the outside world as a sanity check (ping www.cnn.com).

Running the Distribution VM on a Server

The Atrium_2015_A.ova file is simply a tar file containing the disk image (vmdk file) and some configuration (ovf file). Most server virtualization softwares can directly run the vmdk file. However, most people prefer to run qcow2 format in servers. First, untar the ova file

```
$ tar xvf Atrium_2015_A.ova
```

Use the following command to convert the vmdk file to qcow2. Then, the virtualization software can be used to create a VM using gcow2 image.

```
$ qemu-img convert -f vmdk Atrium_2015_A-disk1.vmdk -O qcow2 Atrium_2015_A-disk1.qcow2
```

Running the Distribution VM on the Switch

While it should be possible to run the controller and other software that is part of the distribution VM directly on the switch CPU in a linux based switch OS, it is not recommended. This VM has not been optimized for such an installation, and it has not been tested in such a configuration.

Installation Steps

Once user has the VM up and running, the following steps will help bring up the system.

User has two choices:

A) Bring up the Atrium Router completely in software and completely self-contained in this VM. In addition, a complete test infrastructure (other routers to peer with, hosts to ping from, etc.) that can be played with (via the router-test.py script) will be provided. Note that when using this setup, software switches emulate hardware pipelines. Head over to the "Running Manual Tests" section on the Test Infrastruture page.

B) Bring up the Atrium Router in hardware, working with one of the seven OpenFlow switches Pica8 has certified to work for Project Atrium. Follow the directions below:

Basically, user needs to configure the controller/app, bring up Quagga, connect it to ONOS (via the router-deploy.py script), and configure the switch that is being worked on to connect it to the controller. The following pages will help with that:

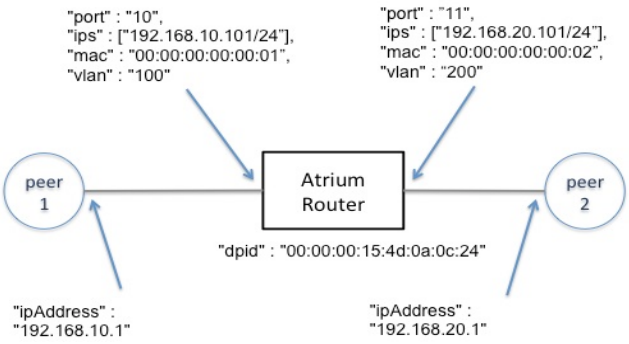
1. Configure and run ONOS
2. Configure and run Quagga
3. Configure Pica8 P-3295

ONOS Configuration Guide

Configuring ONOS

The distribution VM has taken care of most things necessary to configure and run ONOS. What still needs to be done is the routing application within ONOS. At this time, Atrium does not support the ability to change configuration at runtime, an issue which is known. Therefore, it is necessary to pre-configure the controller/app with router-interface addresses and expected BGP peers before launching ONOS. For an example configuration, please see the network shown below.

Figure 1



The configuration shown above needs to be entered in addresses.json and sdnip.json.

addresses.json, which is located in the folder Applications/config, is a file mainly used for ARP handling and router interface IP/VLAN config.

Figure 2

```
admin@atrium:~$ cat Applications/config/addresses.json
{
    "addresses" : [
                  {
                      "dpid" : "00:00:00:15:4d:0a:0c:24",
                      "port" : "10",
                      "ips" : ["192.168.10.101/24"],
                      "mac" : "00:00:00:00:00:01",
                      "vlan" : "100"
                      },
                  {
                      "dpid" : "00:00:00:15:4d:0a:0c:24",
                      "port" : "11",
                      "ips" : ["192.168.20.101/24"],
                      "mac" : "00:00:00:00:00:02",
                      "vlan" : "200"
                      }
    ]
}
```

With reference to the topology diagram, the addresses of our router-interfaces are being specified. The "dpid" refers to the OpenFlow datapath-id of the data-plane switch, "port" refers to the data-plane switch port (the OpenFlow port number), "vlan" is one vlan-id configured on that port, "ips" are the set of ip-addresses assigned to that port/vlan, and "mac" is the mac-address assigned to that port.

A few things to note:

- To assign another vlan to the same port, user needs to create another block within the "addresses" array similar to the two shown above.
- The "mac" does not need to be the actual mac address of the physical switch-port. The "mac" does, however, have to be unique because this is what the router uses to reply to ARP-requests for its interface IPs (on that vlan).
- The "mac" can be the same for all port-vlans. In this case, user is essentially using a single "Router-MAC", which is used to reply to ARP-requests for any interface IP and the source-mac address on all Ethernet frames sent out of this router.
- Most switches do not have any dataplane restrictions on the use of "mac" addresses. However, Pica8 switches **require** the use of a single Router MAC (08:9e:01:82:38:68). See the example config files: Applications/config/pica_addresses.json and Applications/config/pica_sdnip.json

Applications/config/sdnip.json is addressed below.

Figure 3

```
admin@atrium:~$ cat Applications/config/sdnip.json
{

    "bgpPeers" : [
                {
                    "attachmentDpid" : "00:00:00:15:4d:0a:0c:24",
                    "attachmentPort" : "10",
                    "ipAddress" : "192.168.10.1"
                },
                {
                    "attachmentDpid" : "00:00:00:15:4d:0a:0c:24",
                    "attachmentPort" : "11",
                    "ipAddress" : "192.168.20.1"
                }

    ],
    "bgpSpeakers" : [
            {
                 "name" : "bgpSpeaker1",
                 "attachmentDpid" : "00:00:00:00:00:00:00:aa",
                 "attachmentPort" : "1",
                 "macAddress" : "aa:bb:cc:dd:ee:ff",
                 "interfaceAddresses" : [
                                {
                                    "interfaceDpid" : "00:00:00:15:4d:0a:0c:24",
                                    "interfacePort" : "10",
                                    "ipAddress" : "192.168.10.101"
                                },
                                {
                                    "interfaceDpid" : "00:00:00:15:4d:0a:0c:24",
                                    "interfacePort" : "11",
                                    "ipAddress" : "192.168.20.101"
                                }

                    ]

            }

    ]
}
```

"bgpPeers" refers to other routers connected to our Atrium router. These peers can be traditional routers or other Atrium routers. "bgpSpeakers" refers to our Atrium router (i.e there is only one bgpSpeaker).

For the "bgpPeers", the app needs to know two things: the IP address of the peer's interface and where it is attached on the Atrium router. In the example above, for peer1, the IP address of the peer's interface is 192.168.10.1, and it is attached to the Atrium router (attachmentDpid: "00:00:00:15:4d:0a:0c:24") on port 10.

For the "bgpSpeakers", the app needs to know the Atrium router's interface IP addresses in the "interfaceAddresses" section. (Do not change information under "bgpSpeakers" like "attachmentDpid" and "attachmentPort".)

Then, ONOS configuration is complete.

Launching ONOS for a Test

If launching ONOS for testing, user can run the following command from the shell (over ssh). If deploying the router, however, user should follow the instructions below.

To ensure that there are no remaining processes left over from previous runs, please run "./router-cleanup.sh".

Figure 4

```
admin@atrium:~$ ./router-cleanup.sh
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
***  Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
( ip link del sw1-eth4;ip link del as6sw-eth2;ip link del rootTestOn-eth0;ip link del swTestOn-eth1 ) 2> /dev/null
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
admin@atrium:~$
```

ONOS may already be running. Use the following command to ensure that ONOS has not started automatically.

```
admin@atrium:~$ onos-service localhost stop
```

Then, to launch, run "ok clean" (onos-service start/stop can also be used to launch ONOS.)

Figure 5

```
admin@atrium:~$ ok clean
Creating local cluster configs for IP 127.0.0.1...
Staging builtin apps...
Customizing apps to be auto-activated: drivers,openflow,proxyarp,bgprouter...
Welcome to Open Network Operating System (ONOS)!
    ____  _  ______  ____
   / __ \/ |/ / __ \/ __/
  / /_/ /    / /_/ /\ \
  \____/_/|_/\____/___/

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.

onos>
```

To check, enter the command "log:tail" on the ONOS (karaf) CLI.

```
onos> log:tail
```

Scroll through the log and verify that the lines, like those in the figure below, can be seen.

Figure 6

```
2015-06-25 17:18:52,483 | INFO  | FelixStartLevel  | RoutingConfigurationImpl         | 166 - org.onosproject.onos-app-routing - 1.2.0.SNAPSHOT | Routing configuration service started
2015-06-25 17:18:52,495 | INFO  | FelixStartLevel  | BgpRouter                        | 165 - org.onosproject.onos-app-bgprouter - 1.2.0.SNAPSHOT | Router dpid: of:000000154d0a0c24
2015-06-25 17:18:52,495 | INFO  | FelixStartLevel  | BgpRouter                        | 165 - org.onosproject.onos-app-bgprouter - 1.2.0.SNAPSHOT | Control Plane OVS dpid: of:00000000000000aa
2015-06-25 17:18:52,502 | DEBUG | FelixStartLevel  | BgpSessionManager                | 166 - org.onosproject.onos-app-routing - 1.2.0.SNAPSHOT | BGP Session Manager start.
2015-06-25 17:18:52,537 | INFO  | FelixStartLevel  | BgpRouter                        | 165 - org.onosproject.onos-app-bgprouter - 1.2.0.SNAPSHOT | BgpRouter started
```

The "Router dpid" should be the one the user just configured in the config files. The "Control Plane OVS dpid" will be explained in the next section.

User is now ready to configure Quagga.

Launching ONOS for Deployment

For deployment, it is best to launch ONOS within a terminal multiplexer like tmux because, among other things, tmux gives user the ability to maintain persistent working state on remote servers (in our case, on the distribution VM) while detaching and re-attaching at will.

For more on tmux, please see this tutorial.

While still connected via ssh into the distribution VM and having already configured the controller but before ONOS is launched, user should enter

```
admin@atrium:~$ tmux new
```

This command should bring up a window like the one shown below. Notice the "bar" at the bottom, identifying the tmux session.

Figure 7

```
RTNETLINK answers: File exists
admin@atrium:~$ ok clean
Creating local cluster configs for IP 127.0.0.1...
Staging builtin apps...
Customizing apps to be auto-activated: drivers,openflow,proxyarp,bgprouter...
Welcome to Open Network Operating System (ONOS)!
    ____  _  ______  ____
   / __ \/ |/ / __ \/ __/
  / /_/ /    / /_/ /\ \
  \____/_/|_/\____/___/

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.

onos>
```

Now, user can enter "ok clean" to launch ONOS (after running "./router-cleanup.sh" and possibly "onos-service localhost stop").

To detach from the window, enter 'Ctrl-b' followed by 'd'.

User can view the active tmux windows by typing:

```
admin@atrium:~$ tmux ls
0: 1 windows (created Thu Jun 25 17:39:27 2015) [109x36]
```

To reattach to the session:

```
admin@atrium:~$ tmux at -t 0
```

User is now ready to configure Quagga.

Quagga Configuration Guide

Configuring Quagga BGP & Connecting to ONOS

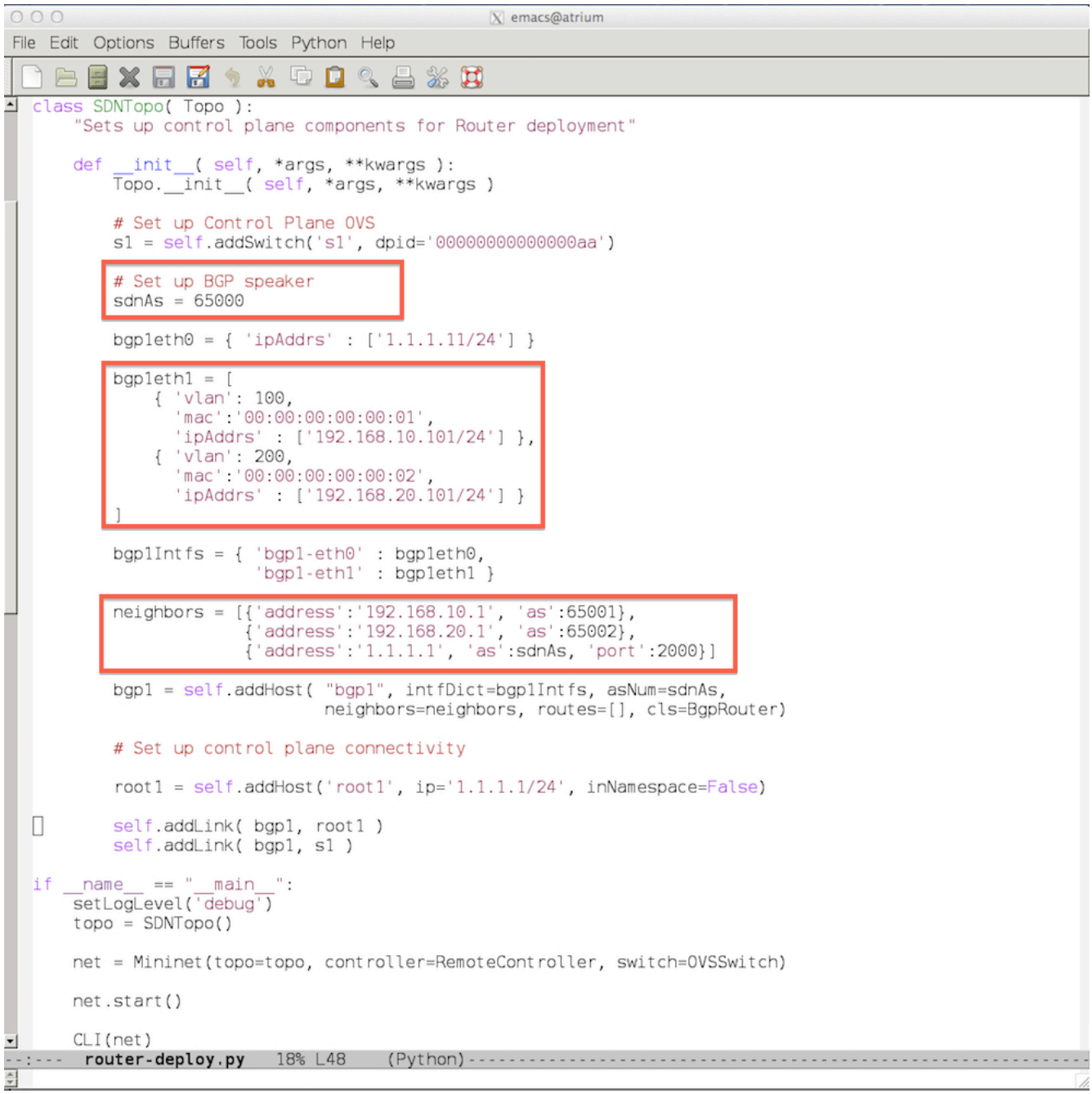
Quagga comes with a rich (Cisco-like) CLI. However, it is not enough to simply configure Quagga BGP. We also need to configure Zebra, as well as the Linux-host on which Quagga runs. In addition, we need to hook up Quagga to ONOS in the control plane. This hookup happens on two different fronts: 1) where BGP communication from the data-plane hardware switch is delivered to ONOS, which in-turn delivers those packets to Quagga (and the reverse communication); and 2) where the ONOS lightweight BGP implementation peers with Quagga BGP using iBGP.

Sounds complicated! But part of Project Atrium's goal is to make life easier for the end user. And so, we have created a script that users can modify in a couple of places and launch with one command that would take care of all the pieces above. If interested in understanding the underlying plumbing, user should refer to the System Architecture.

The script resides at the top level of the directory structure in the distribution VM: **router-deploy.py**

Here is what it looks like:

Figure 1



The highlighted boxes in the script above show what user needs to change for the network:

1. The Atrium Router speaks BGP, so it must have an AS number. Set the AS number in the first box.

2. The second box is where user configures the same interface addresses (mac/vlan/ip) for the Atrium Router as was done when configuring ONOS. Note that there is no need to configure "port" information here. Also note that if user had configured the same mac address for all ports (eg. the RouterMAC case for Pica8 switches), the same would need to be done here.
3. The third box is where user configures the peer's (also called neighbor) IP address and AS number. Do not change the last line in this box: it refers to the ONOS iBGP peer.

User may have noticed that step#2 could be done using Linux commands, and steps 1 and 3 can be done using the Quagga CLI. User may also have noticed that we did not give the ability to advertise routes (also known as 'networks' in BGP terminology). This is a known issue with the Atrium router implementation, an issue which will be addressed in the next release. For this release, the Atrium router can only be used in transit, ie. it can receive and readvertise routes, but it cannot originate route advertisements itself.

Launching Quagga

Similar to what was shown in the "Launching ONOS" section, quagga can be launched simply by running the command in bash (over ssh) if it is just to be run for testing. For deployment, it is better to use tmux and launch quagga in a separate tmux window/pane.

In this example, a new "pane" to launch Quagga was created in the same tmux "window" where ONOS was launched.

In bash, listing the current tmux session should show what was created for launching ONOS.

```
$ tmux ls
0: 1 windows (created Thu Jun 25 17:39:27 2015) [109x36]
```

Attach to the session:

```
$ tmux at -t 0
```

That should bring up the window where ONOS was launched.

Enter the keys Ctrl-b followed by " (double quotation mark). This command will split the window vertically into two panes.

In the lower pane, start the script user just edited in the background.

```
$ sudo ./router-deploy.py &
```

As a checkpoint, user should see the following responses when checking the following commands.

Figure 2

```
admin@atrium:~$ ps aux | grep mininet
root      7474  0.0  0.0  21168  2156 pts/4    Ss+  17:09   0:00 bash --norc -is mininet:c0
root      7480  0.1  0.0  21168  2156 pts/5    Ss+  17:09   0:00 bash --norc -is mininet:bgp1
root      7486  0.0  0.0  21168  2160 pts/6    Ss+  17:09   0:00 bash --norc -is mininet:root1
root      7492  0.0  0.0  21168  2156 pts/7    Ss+  17:09   0:00 bash --norc -is mininet:s1
admin     7627  0.0  0.0  11736   932 pts/3    S+   17:09   0:00 grep --color=auto mininet
```

Here, "bgp1" represents the linux-host (container) that runs Quagga. User can enter this host with:

```
$ ./mininet/util/m bgp1
```

Then, user can telnet into the Quagga BGP process with:

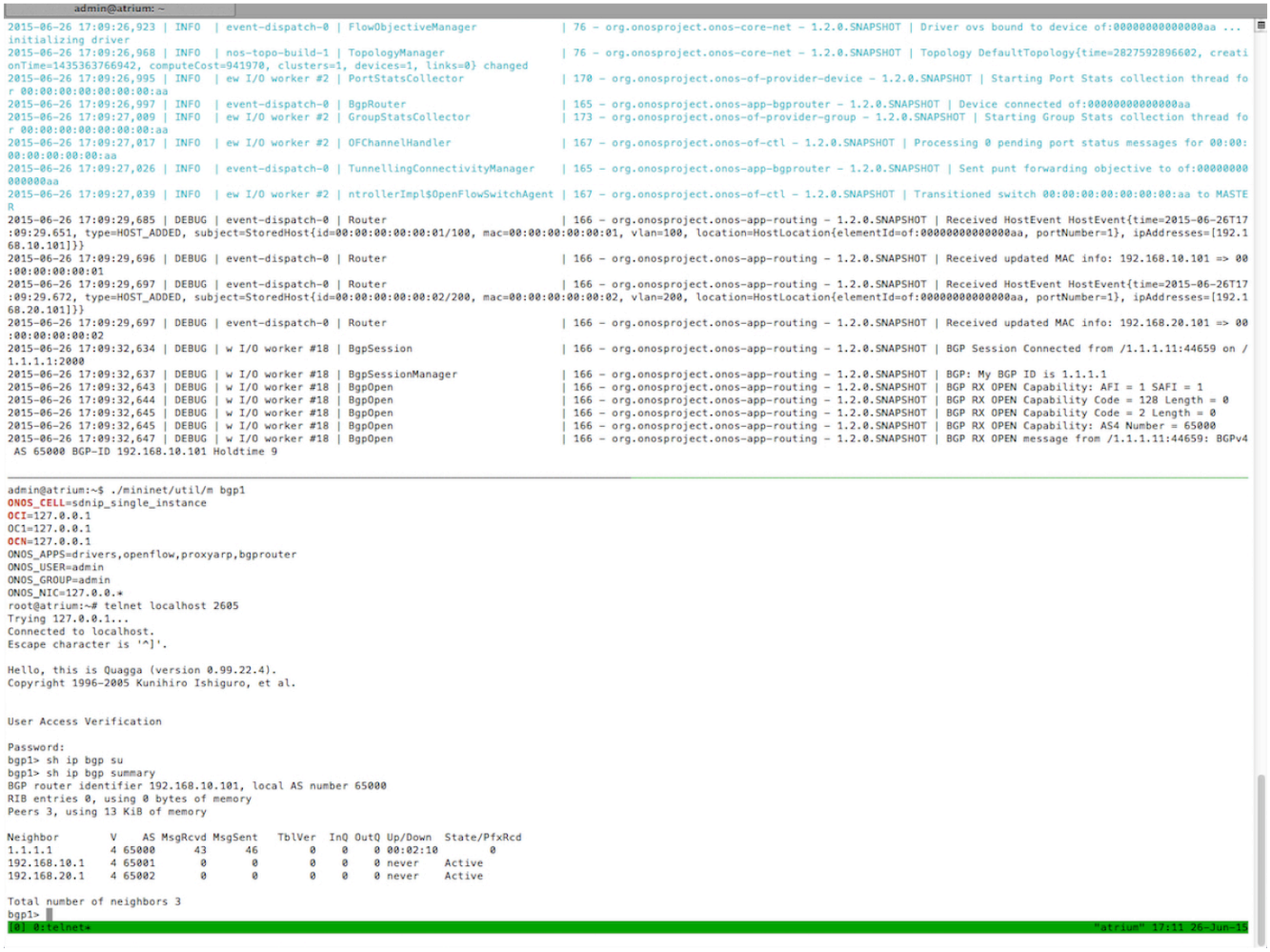
```
$ telnet localhost 2605
```

password: **sdnip**

Now user is in the Quagga CLI. To see the status of BGP peering, enter:

```
> show ip bgp summary
```

Figure 3



The screenshot above shows that the iBGP peering session between ONOS (1.1.1.1) and Quagga is up. The screenshot also shows that the BGP peering session with the neighbors (peers) is not up. This display is due to the fact that the dataplane switch and controller have not been connected.

User is now ready to connect a switch of choice to the controller.

PicOS Configuration Guide

Configuration & Launch

Atrium Specific Configuration

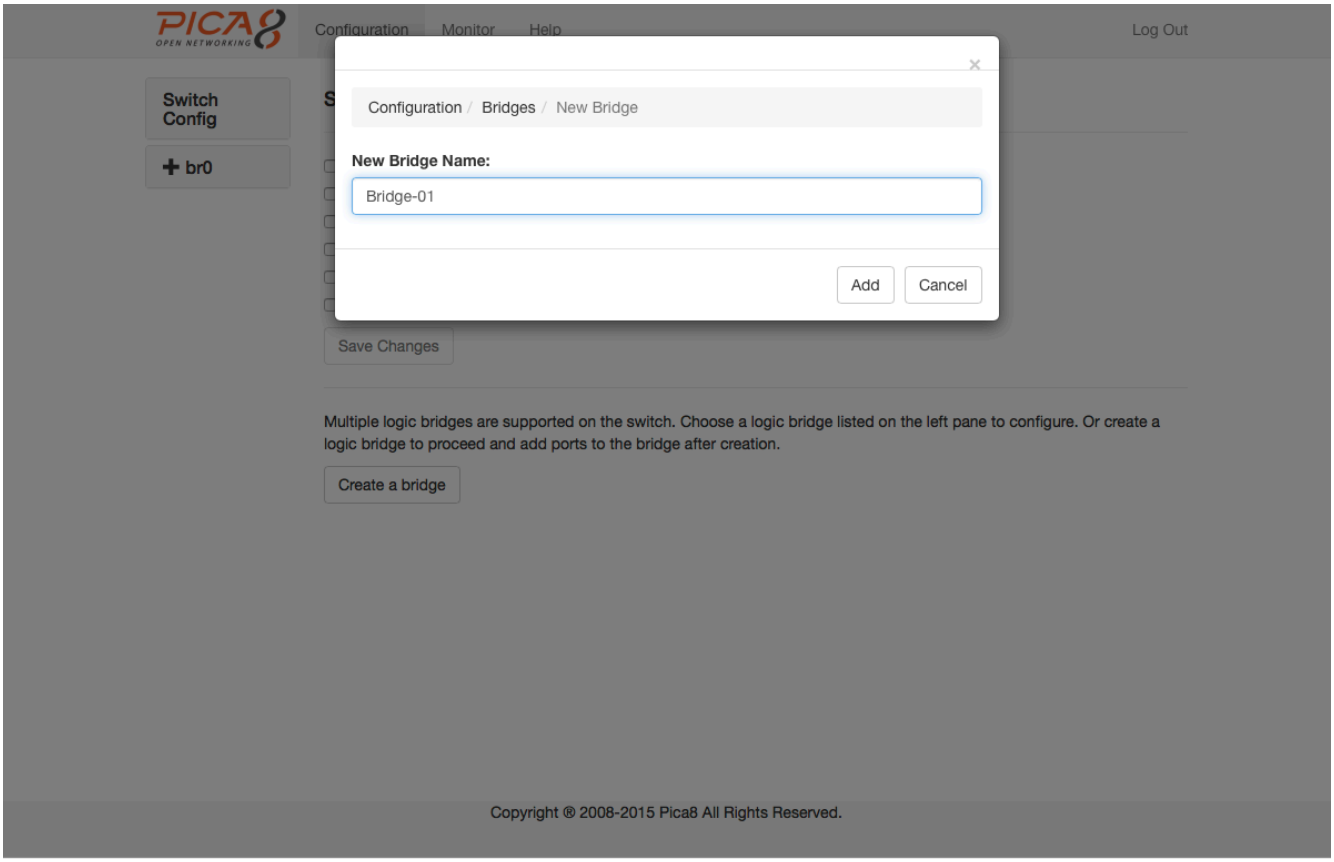
1. Enable multi-table on PicOS. Table 252 is the FDB for IP entries. The preference setting instructs the switch to prioritize match on FDB entries over TCAM.

```
admin@PicOS-OVS$ ovs-vsctl set-l3-mode TRUE 252
admin@PicOS-OVS$ ovs-vsctl set-l2-l3-preference TRUE
```

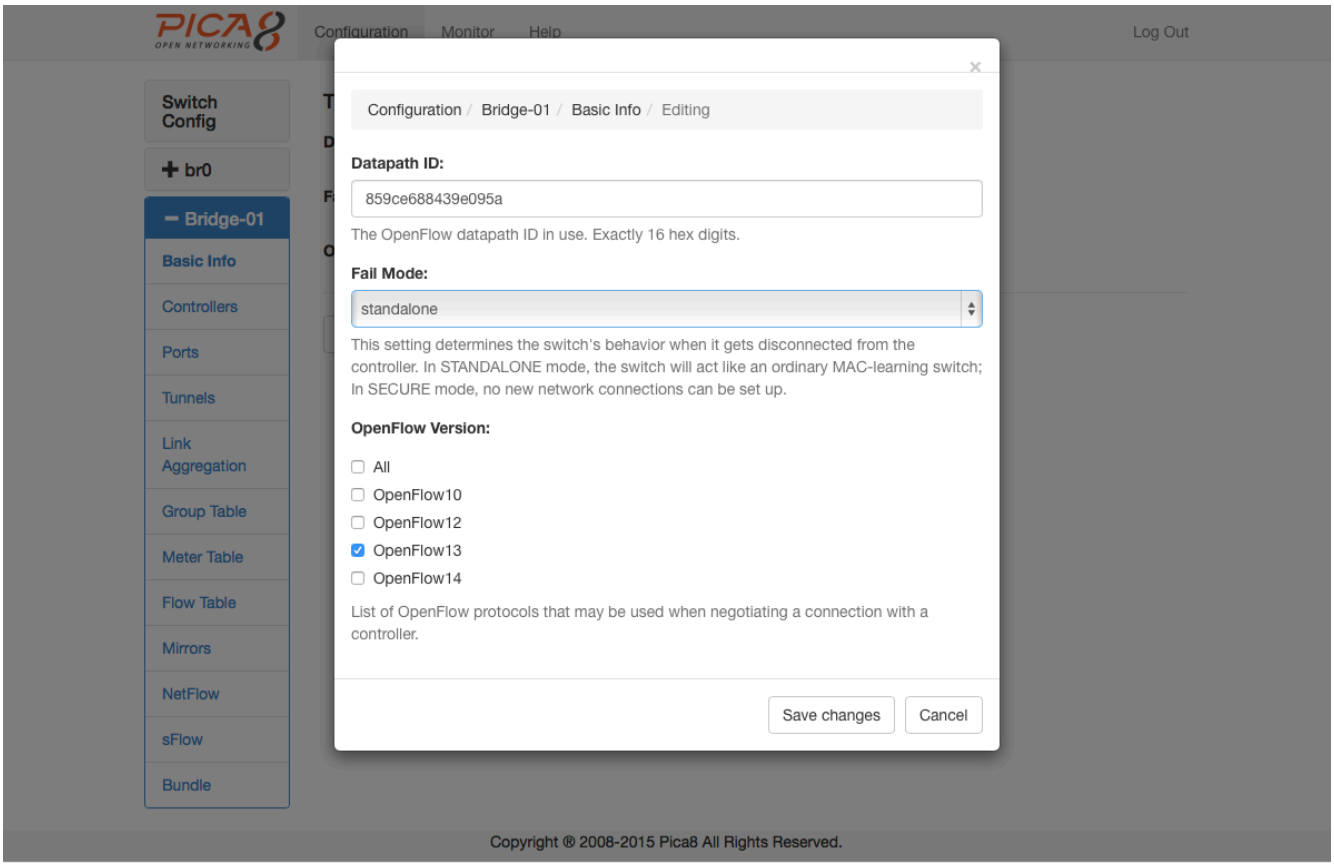
Verify multi-tables are enabled.

```
 admin@PicOS-OVS$ovs-vsctl show-l2-l3-preference
  l2/l3 flow preference is enabled
admin@PicOS-OVS$ovs-vsctl show-l3-mode
  l3 mode is enabled, table id is 252
```

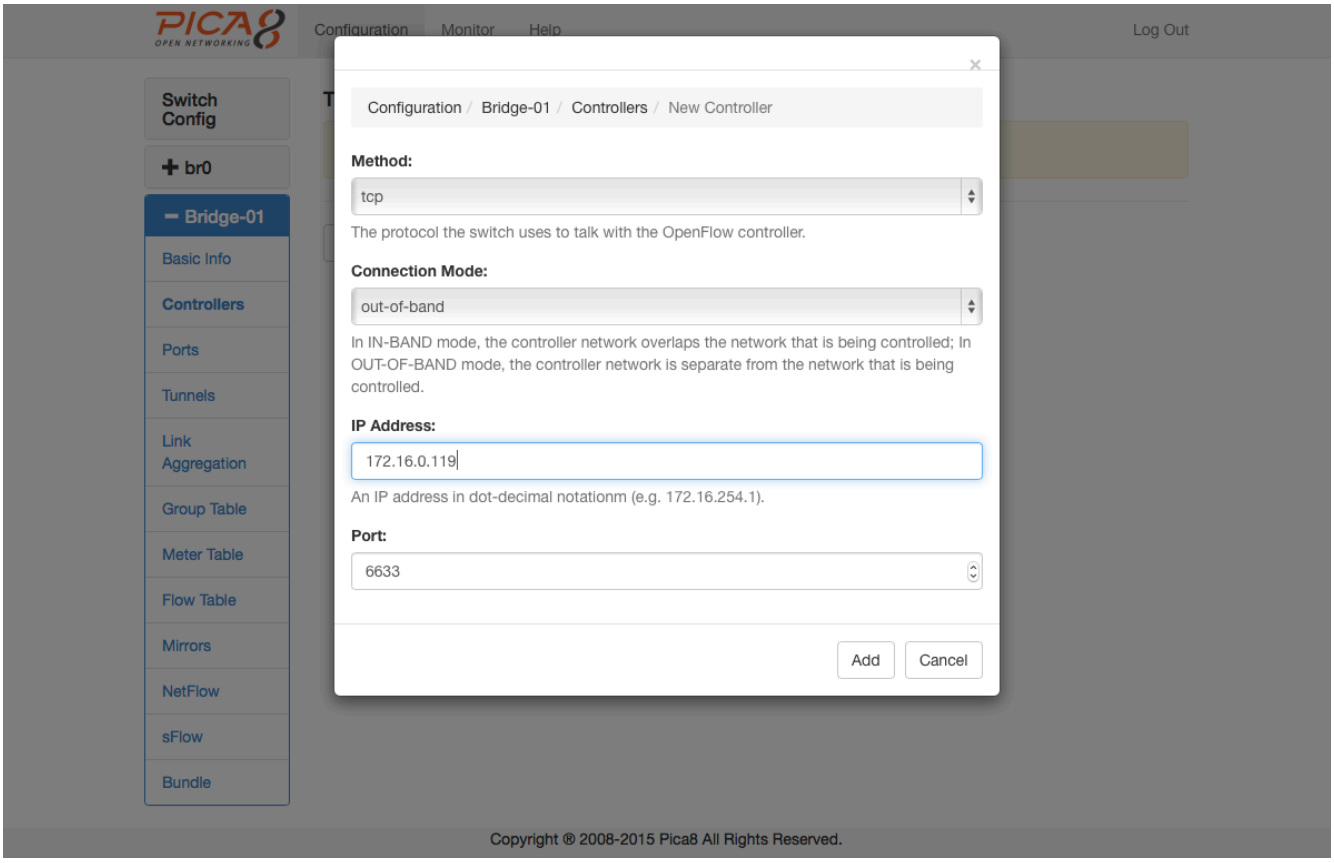
2. Next, create a bridge. Using the GUI is the easiest way: point a browser to the switch management port IP address, use the configuration tab, click on the "Create a bridge" button, and give the bridge a name.



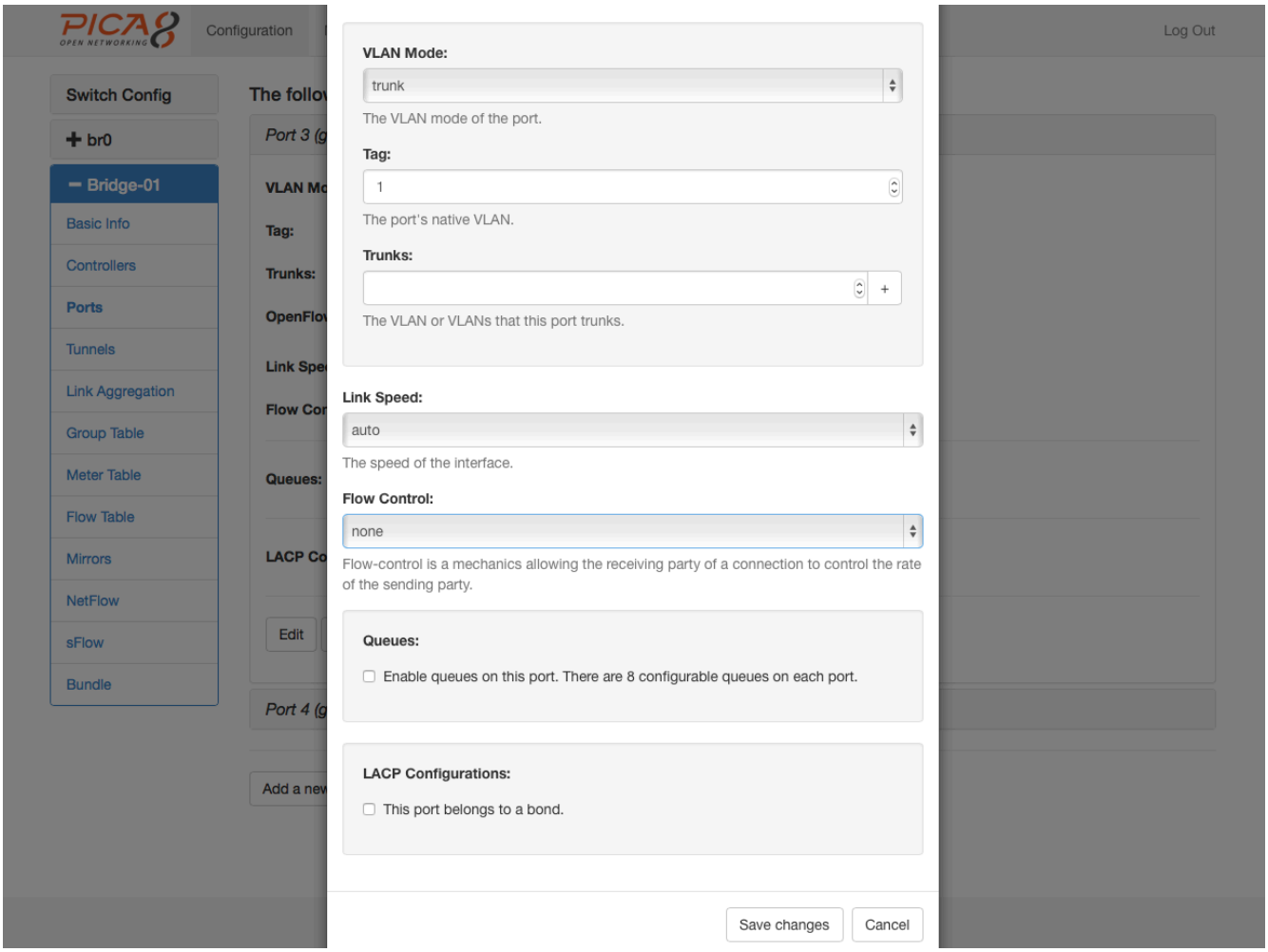
3. Click on the newly created bridge and then "Basic Info". Hit the Edit button. Give a Datapath ID (same one configured in ONOS). Select OpenFlow version 13. The fail mode does not matter.



4. Add a new controller: tcp, out-of-band, <controller-IP> and port 6633



5. Add as many ports as wanted to the bridge. Select the port number. Select TRUNK mode (important). Don't worry about the Tag/Trunk and there is no Flow Control.



Step 6: Finally, remember to use the routerMac: 08:9e:01:82:38:68 for all ports when doing configuration in the controller (in addresses.json and router-deploy.py)

Step 7: Verify the appropriate flows have been installed

```
admin@PicOS-OVS$ovs-ofctl dump-flows atrium-br0
OFPST_FLOW reply (OF1.3) (xid=0x2):
 cookie=0x20000001fc94a5, duration=524.485s, table=0, n_packets=n/a, n_bytes=3648, send_flow_rem priority=65535,arp,in_port=20,dl_vlan=200,dl_dst=ff:ff:ff:ff:ff:ff
actions=CONTROLLER:65535
 cookie=0x20000001faf7b7, duration=524.485s, table=0, n_packets=n/a, n_bytes=4480, send_flow_rem priority=65535,arp,in_port=10,dl_vlan=100,dl_dst=ff:ff:ff:ff:ff:ff
actions=CONTROLLER:65535
 cookie=0x200000af77601b, duration=524.485s, table=0, n_packets=n/a, n_bytes=1664, send_flow_rem priority=65535,arp,in_port=20,dl_vlan=200,dl_dst=08:9e:01:82:38:68
actions=CONTROLLER:65535
 cookie=0x200000af75c32d, duration=524.485s, table=0, n_packets=n/a, n_bytes=2688, send_flow_rem priority=65535,arp,in_port=10,dl_vlan=100,dl_dst=08:9e:01:82:38:68
actions=CONTROLLER:65535
 cookie=0x200000cb4a300f, duration=524.527s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=0 actions=drop
 cookie=0x150000c20cbda8, duration=524.485s, table=0, n_packets=n/a, n_bytes=280738, send_flow_rem priority=65535,ip,in_port=20,dl_vlan=200,dl_dst=08:9e:
01:82:38:68,nw_dst=192.168.20.101 actions=CONTROLLER:65535
 cookie=0x150000c17e35b0, duration=524.485s, table=0, n_packets=n/a, n_bytes=274262, send_flow_rem priority=65535,ip,in_port=10,dl_vlan=100,dl_dst=08:9e:
01:82:38:68,nw_dst=192.168.10.101 actions=CONTROLLER:65535
 cookie=0x150000000e1781, duration=9.026s, table=252, n_packets=n/a, n_bytes=n/a, send_flow_rem priority=220,ip,dl_vlan=100,dl_dst=08:9e:
01:82:38:68,nw_dst=1.0.0.0/24 actions=set_field:08:9e:01:82:38:68->eth_src,set_field:00:90:0b:1f:04:8b->eth_dst,set_field:4196->vlan_vid,output:10
 cookie=0x150000000e1781, duration=9.064s, table=252, n_packets=n/a, n_bytes=n/a, send_flow_rem priority=220,ip,dl_vlan=200,dl_dst=08:9e:
01:82:38:68,nw_dst=1.0.0.0/24 actions=set_field:08:9e:01:82:38:68->eth_src,set_field:00:90:0b:1f:04:8b->eth_dst,set_field:4196->vlan_vid,output:10
 cookie=0x150000000e1781, duration=427.557s, table=252, n_packets=n/a, n_bytes=n/a, send_flow_rem priority=220,ip,dl_vlan=200,dl_dst=08:9e:
01:82:38:68,nw_dst=2.0.0.0/24 actions=set_field:08:9e:01:82:38:68->eth_src,set_field:00:90:0b:23:7d:17->eth_dst,set_field:4296->vlan_vid,output:20
 cookie=0x150000000e1781, duration=427.558s, table=252, n_packets=n/a, n_bytes=n/a, send_flow_rem priority=220,ip,dl_vlan=100,dl_dst=08:9e:
01:82:38:68,nw_dst=2.0.0.0/24 actions=set_field:08:9e:01:82:38:68->eth_src,set_field:00:90:0b:23:7d:17->eth_dst,set_field:4296->vlan_vid,output:20
```

How to Install ONOS

Open Network Operating System (ONOS) is an open source network operating system for software-defined networks (SDN). Intended to run on white box switches, ONOS is targeted at mission critical networks, including service providers. It provides benefits including:

- Virtually unlimited control plane scalability
- High performance, suitable for large network operators
- Mission-critical level of resiliency
- Support for legacy devices
- Next-generation device support and control for devices that support OpenFlow and P4

ONOS is intended to help service providers migrate their existing networks to white box switches, thus lowering CapEx and OpEx. It was developed in conjunction with service providers including AT&T and NTT Communications.

This document describes how to install ONOS.

INSTALLING ONOS :-

1) INSTALL GIT CORE

$ sudo apt-get install git-core

2) ONOS REQUIREMENTS

System requirements

- 2GB or more RAM (I personally recommend at least 4GB)
- 2 or more processors
- Ubuntu 14.04 LTS or 16.04 LTS (Checked with both distros)

3) INSTALL MAVEN AND KARAF

Software requirements

i) Maven

Install Maven 3.3.9 on your Applications directory

$ cd ~

$ mkdir Applications

$ wget http://archive.apache.org/dist/maven/maven-3/3.3.9/binaries/apache-maven-3.3.9-bin.tar.gz

$ tar -zxvf apache-maven-3.3.9-bin.tar.gz -C ../Applications/

NOTE: Although ONOS has been migrated to Buck, maven was used in earlier releases.

ii) Karaf

Install Karaf 3.0.5 on your Applications directory

$ cd ~

$ cd Applications

$ wget http://archive.apache.org/dist/karaf/3.0.5/apache-karaf-3.0.5.tar.gz

$ tar -zxvf apache-karaf-3.0.5.tar.gz -C ../Applications/

4) INSTALL JAVA 8 and set JAVA_HOME

i) Java 8

$ sudo apt-get install software-properties-common -y

$ sudo add-apt-repository ppa:webupd8team/java -y

$ sudo apt-get update

$ sudo apt-get install oracle-java8-installer oracle-java8-set-default -y

ii) SET YOUR JAVA_HOME

$ export JAVA_HOME=/usr/lib/jvm/java-8-oracle

iii) VERIFY IT WITH FOLLOWING COMMAND

$ env | grep JAVA_HOME

JAVA_HOME=/usr/lib/jvm/java-8-oracle

5) DOWNLOAD THE LATEST ONOS

$ git clone https://gerrit.onosproject.org/onos

$ cd onos

$ git checkout master

6) ENVIRONMENTAL VARIABLES

The ONOS source comes with a sample bash_profile that can set these variables for you.

i) Edit ~/.bashrc

$ nano ~/.bashrc

ii) Add the following line at the end

. ~/onos/tools/dev/bash_profile

iii) Reload .bashrc or log out and log in again to apply the changes

. ~/.bashrc

iv) Once you run the above command, you will see in the output of the env command that several new variables, such as ONOS_ROOT, MAVEN, and KARAF_ROOT, have been set.

$ env | grep ONOS_ROOT

ONOS_ROOT=/Users/nirmalkaria/onos

$ env | grep MAVEN

MAVEN=/Users/nirmalkaria/Applications/apache-maven-3.3.9

$ env | grep KARAF_ROOT

KARAF_ROOT=/Users/nirmalkaria/Applications/apache-karaf-3.0.8

7) BUILD AND DEPLOY ONOS

i) Edit ~/Applications/apache-karaf-3.0.5/etc/org.apache.karaf.features.cfg file by appending the following line to featuresRepositories:

$ nano ~/Applications/apache-karaf-3.0.5/etc/org.apache.karaf.features.cfg

ii) Locate the featuresRepositories and append this line (will need a comma before appending the text to separate from the previous value)

mvn:org.onosproject/onos-features/1.10.0-SNAPSHOT/xml/features

8) BUILD ONOS WITH MAVEN

$ cd ~/onos

$ mvn clean install or use the alias 'mci'

9) Selecting IP address

Export ONOS4_IP or ONOS_NIC environment variables with the IP address prefix to configure ONOS clustering component. This IP address is the ip address of the controller.

$ export ONOS_IP=10.1.9.255

$ export ONOS_NIC=10.1.9.*

10) Selecting ONOS apps to activate

To configure ONOS with a set of applications that should be automatically activated on startup, use the ONOS_APPS environment variable as follows:

$ export ONOS_APPS=drivers,openflow,proxyarp,mobility,fwd

11) Starting ONOS

```
$ ok clean
Creating local cluster configs for IP 10.1.9.247...
Setting up hazelcast.xml for subnet 10.1.9.*...
Staging builtin apps...
Customizing apps to be auto-activated: drivers,openflow,proxyarp,mobility,fwd...
Welcome to Open Network Operating System (ONOS)!

    ____  _  _______  ____
   / __ \/ |/ / __ \/ __/
  / /_/ /    / /_/ /\ \
  \____/_/|_/\____/___/

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.
onos>
```

At this point, typing help onos at the prompt should still bring up a list of available commands. Pressing **Ctrl-D** or logout will exit the CLI.

METHOD 2

BUILDING ONOS USING BUCK

1) INSTALL JAVA 8 and set JAVA_HOME

i) Java 8

$ sudo apt-get install software-properties-common -y

$ sudo add-apt-repository ppa:webupd8team/java -y

$ sudo apt-get update

$ sudo apt-get install oracle-java8-installer oracle-java8-set-default -y

ii) SET YOUR JAVA_HOME

$ export JAVA_HOME=/usr/lib/jvm/java-8-oracle

iii) Verify it with the following command

$ env | grep JAVA_HOME

JAVA_HOME=/usr/lib/jvm/java-8-oracle

2) Download latest ONOS

$ git clone https://gerrit.onosproject.org/onos

$ cd onos

$ git checkout master

3) Development Environment Setup

The ONOS_ROOT environment variable is exported in the shell profile (.bash_aliases, .profile, etc.)

$ export ONOS_ROOT=~/onos

$ source $ONOS_ROOT/tools/dev/bash_profile

4) Build with Buck

$ sudo apt-get install zip unzip

$ cd $ONOS_ROOT

$ tools/build/onos-buck build onos --show-output

```
Vineels-MacBook-Air:onos nirmalkaria$  tools/build/onos-buck build onos --show-output

Not using buckd because NO_BUCKD is set.
[-] PROCESSING BUCK FILES...FINISHED 5.2s [100%] 🐳 New buck daemon
[+] DOWNLOADING... (0.00 B/S, TOTAL: 0.00 B, 0 Artifacts)
[+] BUILDING...14.3s [15%] (208/209 JOBS, 1 UPDATED, 1 [0.5%] CACHE MISS)
 |=> IDLE
 |=> IDLE
 |=> //tools/package:onos-package...  1.5s (checking local cache)
 |=> IDLE
The outputs are:
//tools/package:onos-package buck-out/gen/tools/package/onos-package/onos.tar.gz
```

ii) To execute ONOS unit tests,

$ tools/build/onos-buck test

```
Vineels-MacBook-Air:onos nirmalkaria$ tools/build/onos-buck test
Not using buckd because NO_BUCKD is set.
[-] PROCESSING BUCK FILES...FINISHED 1.0s [100%] 🐳 New buck daemon
[-] PROCESSING BUCK FILES...FINISHED 1.0s [100%] 🐳 New buck daemon
[-] DOWNLOADING... (0.00 B/S AVG, TOTAL: 0.00 B, 0 Artifacts)
[-] BUILDING...FINISHED 2m15.7s [100%] (1487/1487 JOBS, 1060 UPDATED, 767 [51.6%
[-] TESTING...FINISHED 3m40.5s (5378 PASS/0 FAIL)
RESULTS FOR ALL TESTS
PASS       8.1s  1 Passed   0 Skipped   0 Failed   //apps/acl:onos-apps-acl-checkstyle-files-checkstyle
NOTESTS <100ms  0 Passed   0 Skipped   0 Failed   org.onosproject.acl.AclWebResourceTest
PASS       3.4s  1 Passed   0 Skipped   0 Failed   //apps/acl:onos-apps-acl-tests-checkstyle
PASS       8.1s  1 Passed   0 Skipped   0 Failed   //apps/actn-mdsc/tetunnel-ctl:onos-apps-actn-mdsc-tetunnel-ctl-checkstyle-files-checkstyle
PASS       6.0s  1 Passed   0 Skipped   0 Failed   //apps/actn-mdsc/tetunnel-pce:onos-apps-actn-mdsc-tetunnel-pce-checkstyle-files-checkstyle
PASS     798ms  1 Passed   0 Skipped   0 Failed   //apps/bgprouter:onos-apps-bgprouter-checkstyle-files-checkstyle
PASS       1.1s  1 Passed   0 Skipped   0 Failed   //apps/castor:onos-apps-castor-checkstyle-files-checkstyle
PASS     723ms  1 Passed   0 Skipped   0 Failed   //apps/cip:onos-apps-cip-checkstyle-files-checkstyle
PASS       1.2s  1 Passed   0 Skipped   0 Failed   //apps/config:onos-apps-config-checkstyle-files-checkstyle
PASS     769ms  1 Passed   0 Skipped   0 Failed   //apps/cord-support:onos-apps-cord-support-checkstyle-files-checkstyle
PASS       1.2s  1 Passed   0 Skipped   0 Failed   //apps/cpman/api:onos-apps-cpman-api-checkstyle-files-checkstyle
PASS    <100ms  2 Passed   0 Skipped   0 Failed   org.onosproject.cpman.message.ControlMessageEventTest
PASS    <100ms  2 Passed   0 Skipped   0 Failed   org.onosproject.cpman.message.DefaultControlMessageTest
PASS     869ms  1 Passed   0 Skipped   0 Failed   //apps/cpman/api:onos-apps-cpman-api-tests-checkstyle
PASS       1.4s  1 Passed   0 Skipped   0 Failed   //apps/cpman/app:onos-apps-cpman-app-checkstyle-files-checkstyle
```

iii) To import the project into IntelliJ

$ tools/build/onos-buck project

```
Vineels-MacBook-Air:onos nirmalkaria$ tools/build/onos-buck project
Not using buckd because NO_BUCKD is set.
OK   //lib:netty-common-4.1.5.Final.jar MATCHING_RULE_KEY buck-out/gen/lib/netty
-common-4.1.5.Final.jar/netty-common-4.1.5.Final.jar
OK   //lib:asm-5.0.4.jar MATCHING_RULE_KEY buck-out/gen/lib/asm-5.0.4.jar/asm-5.
0.4.jar
OK   //lib:commons-collections-3.2.2.jar MATCHING_RULE_KEY buck-out/gen/lib/comm
ons-collections-3.2.2.jar/commons-collections-3.2.2.jar
OK   //lib:commons-configuration-1.10.jar MATCHING_RULE_KEY buck-out/gen/lib/com
mons-configuration-1.10.jar/commons-configuration-1.10.jar
OK   //lib:commons-io-2.4.jar MATCHING_RULE_KEY buck-out/gen/lib/commons-io-2.4.
jar/commons-io-2.4.jar
OK   //lib:commons-lang-2.6.jar MATCHING_RULE_KEY buck-out/gen/lib/commons-lang-
2.6.jar/commons-lang-2.6.jar
OK   //lib:commons-lang3-3.5.jar MATCHING_RULE_KEY buck-out/gen/lib/commons-lang
```

5) Run ONOS

$ cd $ONOS_ROOT

$ tools/build/onos-buck run onos-local -- clean debug

```
Vineels-MacBook-Air:onos nirmalkaria$  tools/build/onos-buck run onos-local -- c
lean debug

Not using buckd because NO_BUCKD is set.
[-] PROCESSING BUCK FILES...FINISHED 7.1s [100%] 🐳 New buck daemon
[-] DOWNLOADING... (0.00 B/S AVG, TOTAL: 0.00 B, 0 Artifacts)
[-] BUILDING...FINISHED 38.4s [100%] (210/210 JOBS, 16 UPDATED, 8 [3.8%] CACHE M
Running clean installation...
# Host [localhost]:8101 found: line 30
/Users/nirmalkaria/.ssh/known_hosts updated.
Original contents retained as /Users/nirmalkaria/.ssh/known_hosts.old
Creating local cluster configs for IP 172.16.1.112...
Waiting for karaf.log
Mar 20, 2017 1:58:24 PM org.apache.karaf.main.Main launch
INFO: Installing and starting initial bundles
Mar 20, 2017 1:58:25 PM org.apache.karaf.main.Main launch
INFO: All initial bundles installed and set to start
Mar 20, 2017 1:58:25 PM org.apache.karaf.main.lock.SimpleFileLock lock
INFO: Trying to lock /private/tmp/onos-1.10.0-SNAPSHOT/apache-karaf-3.0.8/lock
Mar 20, 2017 1:58:25 PM org.apache.karaf.main.lock.SimpleFileLock lock
```

i) To attach to the ONOS CLI console, run:

$ tools/test/bin/onos localhost

```
Vineels-MacBook-Air:onos nirmalkaria$ tools/test/bin/onos localhost
Warning: Permanently added '[localhost]:8101' (RSA) to the list of known hosts.
Welcome to Open Network Operating System (ONOS)!
    ____  _  ______  ____
   / __ \/ |/ / __ \/ __/
  / /_/ /    / /_/ /\ \
  \____/_/|_/\____/___/

Documentation: wiki.onosproject.org
Tutorials:     tutorials.onosproject.org
Mailing lists: lists.onosproject.org

Come help out! Find out how at: contribute.onosproject.org

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.

onos>
```

ii) To open your default browser on the ONOS GUI page, simply type:

$ tools/test/bin/onos-gui localhost or alternatively visit http://localhost:8181/onos/ui

Feature Supported in PicOS OVS

- Feature supported in different platform
- Match fields supported

Feature supported in different platform

Model	CPU	RAM	ASIC	ASIC Model	PTP-TC	ovs flow number	mirror number	ipv4(NAT)	ipv6	mpls	l2mpls	gre	l2gre	vxlan	resilient hash	symmetric hash	gtp tei
as4600_54t（4654）	2-core powerpc 1000.000000MHz	2074612 KB	Apllo2	BCM56540	N	4096	4	N	Y	Y	N	Y	N	N	N	N	N
P3295	1-core powerpc 825.000000MHz	515808 KB	Firebolt3	BCM56538	N	2048		N	Y	N	N	Y	N	N	N	N	N
P3296（3297）	2-core powerpc 799.999992MHz	2073452 KB	Triumph2	BCM56634	N	4096		N	Y	Y	N	Y	N	N	N	N	N
P3930	2-core powerpc 799.999992MHz	2073728 KB	Trident+	BCM56846	N	1024		N	N	Y	N	Y	N	N	N	N	N
P3920	2-core powerpc 1200.000000MHz	2073724 KB	Trident+	BCM56846	N	1024		N	N	Y	N	Y	N	N	N	N	N
as5600_52x（3924）	2-core powerpc 799.999992MHz	2074612 KB	Trident+	BCM56846	N	1024		N	N	Y	N	Y	N	N	N	N	N
P3922	2-core powerpc 1000.000000MHz	2072888 KB	Trident+	BCM56846	N	1024		N	N	Y	N	Y	N	N	N	N	N
P5401	2-core powerpc 1200.000000MHz	2073984 KB	Trident2	BCM56850	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
P5101	2-core powerpc 1200.000000MHz	2074612 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
as5712_54x	4-core X86 2400.097MHz	8159248 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
as6701_32x	2-core powerpc 1200.000000MHz	2074612 KB	Trident2	BCM56850	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
P3780	1-core powerpc 999.990000MHz	515796 KB	Trident	BCM56843	N	1024	4	N	N	Y	Y	Y	Y	Y	N	N	N
as4610_54p-poe	2-core arm unknown	765320 KB	Helix4	BCM56340	Y	2048	4	N	Y	N	N	Y	N	N	N	Y	N
Niagara2632XL	8-core X86 2100.040MHz	16324616 KB	Trident2	BCM56850	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Arctica4804i	2-core powerpc 799.999992MHz	2073452 KB	Triumph2	BCM56630	N	4096	4	N	Y	Y	Y	Y	N	N	N	N	N
as6712_32x	4-core X86 2399.998MHz	8145056 KB	Trident2	BCM56850	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
as4610_30t	2-core arm unknown	765320 KB	Helix4	BCM56340	Y	2048	4	N	Y	N	N	Y	N	N	N	Y	N
4048	8-core X86 2700MHz	2000000 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
7712	4-core X86 C2538.2.40GHz	16420208 KB	Tomahawk	BCM56960	Y	1024	4	N	N	Y	Y	Y	Y	Y	N	Y	Y
as5812_54t	8-core X86 C2538 2.40GHz	4194304KB	Trident2Plus	BCM56860	Y	8192	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
as5812_54x	8-core X86 C2538 2.40GHz	4194304KB	Trident2Plus	BCM56860	Y	8192	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
arctica4806xp	8-core X86 2400.097MHz	62914560 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AG9032	4-core X86 2400.097MHz	8138456KB	Tomahawk	BCM56960	Y	1024	4	N	N	Y	Y	Y	Y	Y	N	Y	Y
as7312_54x	4-core X86 2400.099MHz	16403224KB	Tomahawk	BCM56960	Y	1024	4	N	N	Y	Y	Y	Y	Y	N	Y	Y
AG6248-poe	2-core arm 1.0 GHz	1032948KB	Helix4	BCM56340	Y	2048	4	N	Y	N	N	Y	N	N	N	Y	N
Z9100	4-core X86 C2538.2.40GHz	16420208 KB	Tomahawk	BCM56960	Y	1024	4	N	N	Y	Y	Y	Y	Y	N	Y	Y
as4610_30P-poe	2-core arm 1.0 GHz	1032948KB	Helix4	BCM56340	Y	2048	4	N	Y	N	N	Y	N	N	N	Y	N
AG7648	8-core X86 2700MHz	2000000 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AG5648	4-core X86 2400.099MHz	16403224KB	Tomahawk	BCM56960	Y	1024	4	N	N	Y	Y	Y	Y	Y	N	Y	Y
6254	8-core X86 2700MHz	2000000 KB	Trident2	BCM56854	Y	2048	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
6812_32x	8-core X86 C2538 2.40GHz	4194304KB	Trident2Plus	BCM56860	Y	8192	4	Y	N	Y	Y	Y	Y	Y	N	Y	Y
s4148t	1-core X86 C2338.1.7GHz	4194304KB	Maverick	BCM56768	Y	4096	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
AS3000_52P	dual-core ARM CortexA9800MHz	8388608KB	marvell PonCat3	98DX3336	N	768	4	N	N	N	N	Y	N	N	N	N	N
s4148f	1-core X86 C2338.1.7GHz	4194304KB	Maverick	BCM56768	Y	4096	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
s4128f	1-core X86 C2338.1.7GHz	4194304KB	Maverick	BCM56762	Y	4096	4	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

Match fields supported

Match Fields	Disable match-mode	Enable match-mode											
		mac	mac_x	ip	ip_x	ipv4_quintuple	arp_tpa	arp_full	arp_min	l2l4	ipv6_full	ipv6_src	ipv6_dst
table=<number>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
in_port=<port>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
dl_src=<mac[/mask]>	Y	Y	Y	N	N	N	N	Y	N	Y	N	Y	Y
dl_dst=<mac[/mask]>	Y	Y	Y	N	N	N	N	Y	N	Y	N	Y	Y
dl_type=<ethernet type>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
vlan_tci=<tci[/mask]>	Y	N	N	N	N	N	N	N	N	Y	N	N	N
dl_vlan=<vlanid>	Y	Y	Y	N	N	Y	N	Y	N	Y	Y	Y	Y
dl_vlan_pcp=<value>	Y	N	N	N	N	N	N	N	N	Y	N	N	N
arp_spa=ip[/netmask]	Y	N	N	N	N	N	N	Y	Y	N	N	N	N
arp_tpa=ip[/netmask]	Y	N	N	N	N	N	Y	Y	Y	N	N	N	N
arp_sha=<mac[/mask]>	N	N	N	N	N	N	N	N	N	N	N	N	N
arp_tha=<mac[/mask]>	N	N	N	N	N	N	N	N	N	N	N	N	N
arp_op=<opcode>	Y	N	N	N	N	N	N	Y	Y	N	N	N	N
nw_src=ip[/netmask]	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
nw_dst=ip[/netmask]	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	N	Y
nw_proto=<proto> ip_proto=<proto>	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
nw_tos=<tos>	Y	N	N	N	N	N	N	N	N	Y	N	N	N
ip_dscp=<dscp>	Y	N	N	N	N	N	N	N	N	Y	N	N	N
nw_ecn=<ecn> ip_ecn=<ecn>	Y	N	N	N	N	N	N	N	N	N	N	N	N
nw_ttl=<value>	Y	N	N	N	N	N	N	N	N	N	N	N	N
tcp_src=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
tcp_dst=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
udp_src=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
udp_dst=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
sctp_src=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
sctp_dst=<port[/mask]>	Y	N	N	Y	Y	Y	N	N	N	Y	Y	N	N
tcp_flags=<flags/mask> tcp_flags=[+flag...][-flag...]	Y	N	N	N	N	N	N	N	N	N	N	N	N
icmp_type=<type>	Y	N	N	N	N	N	N	N	N	N	N	N	N
icmp_code=<code>	Y	N	N	N	N	N	N	N	N	N	N	N	N
ip_frag=<frag_type>	Y	N	N	N	N	N	N	N	N	N	N	N	N
ipv6_src=<ipv6[/netmask] >	Y (Only P3290,P3295,P3296,es4654bf,as4610, ag6248c can support matching it.)	N	N	N	N	N	N	N	N	N	Y	Y	N

ipv6_dst=<ipv6[/netmask] >	Y (Only P3290,P3295,P3296,es4654bf,as4610, ag6248c can support matching it.)	N	N	N	N	N	N	N	N	N	Y	N	Y
ipv6_label=<label>	Y (Only P3290,P3295,P3296,es4654bf,as4610, ag6248c can support matching it.)	N	N	N	N	N	N	N	N	N	Y	Y	Y
nd_target=<ipv6[/netmask]>	N	N	N	N	N	N	N	N	N	N	N	N	N
nd_sll=<mac>	N	N	N	N	N	N	N	N	N	N	N	N	N
nd_tll=<mac>	N	N	N	N	N	N	N	N	N	N	N	N	N

PICOS Open vSwitch Command Reference

Pica8 PicOS software leverages Open vSwitch, a production quality, multi-layer virtual switch licensed under the open source Apache 2.0 license. OVS runs as a process within PicOS. The OpenFlow protocol is driven by the Open Networking Foundation (ONF), a leader in software-defined networking (SDN). The OpenFlow protocol governs three essential components of SDN, including an OpenFlow physical switch, an OpenFlow virtual switch to manage virtual machines, and an OpenFlow controller to organize all network pieces.

Organization

This document presents OVS commands arranged in three major sections:

- **ovs−appctl:** Utility for querying and controlling **ovs-vswitchd** (Open vSwitch daemon)
- **ovs-ofctl:** OpenFlow switch management utility
- **ovs-vsctl:** Utility for configuring and controlling **ovs-vswitchd** (Open vSwitch daemon)

Additional Resources

For detailed information about Open vSwitch, OpenFlow, and command usage, visit the following web sites:

- **Open vSwitch Advanced Features Tutorial**
- **Open vSwitch**
- **OpenFlow**

ovs−appctl Commands

- ovs-appctl Target Commands
- ovs-appctl Common Commands

ovs−ofctl Commands

- ovs-ofctl Common Commands
- ovs-ofctl dump-meters <bridge>

ovs−vsctl Commands

- Bridge Commands
- Port Commands
- Controller commands
- Database commands
- Interface commands
- Mirror Commands
- NetFlow Commands
- Open vSwitch commands
- Match-mode Command
- QoS_queue Commands
- sFlow commands
- Cos-map Command
- Egress-mode Command
- Set-flow-counter-mode Command
- Combinated-mode Command
- DSCP Commands

ovs−appctl Commands

ovs−appctl is a utility for querying and controlling the Open vSwitch daemon.

User can view the **ovs-appctl** help for more information about the utility.

```
admin@Leaf1$ovs-appctl --help
ovs-appctl, for querying and controlling Open vSwitch daemon
usage: ovs-appctl [TARGET] COMMAND [ARG...]
Targets:
  -t, --target=TARGET  pidfile or socket to contact
Common commands:
  help               List commands supported by the target
  version            Print version of the target
  vlog/list          List current logging levels
  vlog/set [SPEC]
      Set log levels as detailed in SPEC, which may include:
      A valid module name (all modules, by default)
      'syslog', 'console', 'file' (all facilities, by default))
      'off', 'emer', 'err', 'warn', 'info', or 'dbg' ('dbg', bydefault)
  vlog/reopen        Make the program reopen its log file
Other options:
  --timeout=SECS     wait at most SECS seconds for a response
  -h, --help         Print this helpful information
  -V, --version      Display ovs-appctl version information
```

User may also view the ovs-appctl manual page for detailed syntax and additional information.

```
admin@Leaf1$man ovs-appctl
ovs-appctl(8)                Open vSwitch Manual               ovs-appctl(8)
NAME
       ovs-appctl - utility for configuring running Open vSwitch daemons
SYNOPSIS
       ovs-appctl [--target=target | -t target] command [arg...]
       ovs-appctl --help
       ovs-appctl --version
DESCRIPTION
       Open  vSwitch  daemons  accept  certain  commands at runtime to control
       their behavior and query their settings.  Every daemon accepts a common
       set  of  commands documented under COMMON COMMANDS below.  Some daemons
       support  additional  commands  documented  in  their  own  manpages.
       ovs-vswitchd in particular accepts a number of additional commands doc-
       umented in ovs-vswitchd(8).
       The ovs-appctl program provides a simple way to invoke these  commands.
       The  command  to  be  sent is specified on ovs-appctl's command line as
       non-option arguments.  ovs-appctl sends the command and prints the dae-
       mon's response on standard output.
<Some output omitted>
```

.

- ovs-appctl Common Commands
- ovs-appctl Target Commands

ovs-appctl Common Commands

This section includes the common comands of ovs-appctl.

- ovs-appctl Help
- ovs-appctl hwlog/set-level <module> <level>
- ovs-appctl hwlog/set-type <mode> <type>
- ovs-appctl ofproto/set_L34_enable
- ovs-appctl Version
- ovs-appctl vlog/list
- ovs-appctl vlog/set
- Pica8 Commands

ovs-appctl Help

Lists commands supported by the ovs-vswitchd.

ovs-appctl hwlog/set-level <module> <level>

Set hwlog level of <module> as detailed in <level>.
The <module> contains sdk/api/all; the <level> contains debug/info/warn/error|/off.

ovs-appctl hwlog/set-level all debug

Set hwlog level of 'all' module as 'debug'.

ovs-appctl hwlog/set-level sdk debug

Set hwlog level of 'sdk' module as 'debug'.

ovs-appctl hwlog/set-level api debug

Set hwlog level of 'api' module as 'debug'.

ovs-appctl hwlog/set-type <mode> <type>

Enable/disable hwlog of <mode>.
The <mode> contains config/packet/all; the <type> contains true/false.

ovs-appctl hwlog/set-type config true

Enable hwlog of configurations.

ovs-appctl ofproto/set_L34_enable

To control whether or not flows unsupported by the hardware can be added, use the **ovs-appctl ofproto/set_L34_enable** command in OVS mode.

Command Syntax

ovs-appctl ofproto/set_L34_enable { **true** | **false** }

Parameters

true	Flows not supported by hardware can be added. This is the default option.
false	Flows not supported by hardware cannot be added.

ovs-appctl Version

ovs-appctl version

Print the version of the ovs-vswitchd.

Example

```
admin@PicOS-OVS$ovs-appctl version
ovs-vswitchd (Open vSwitch) 2.3.0
Compiled May 27 2015 23:04:41
```

ovs-appctl vlog/list

To list the known logging modules and their current levels, use the **ovs-appctl vlog/list** command.

Syntax

ovs-appctl vlog/list

Parameters

There are no parameters for this command.

Examples

The following example lists the known logging modules and their current levels:

```
admin@Switch$ovs-appctl vlog/list
                 console    syslog    file
                 -------    ------    ------
backtrace         INFO       INFO       INFO
bfd               INFO       INFO       INFO
bond              INFO       INFO       INFO
bridge            INFO       INFO       INFO
bundle            INFO       INFO       INFO
bundles           INFO       INFO       INFO
cfm               INFO       INFO       INFO
classifier        INFO       INFO       INFO
collectors        INFO       INFO       INFO
command_line      INFO       INFO       INFO
connmgr           INFO       INFO       INFO
coverage          INFO       INFO       INFO
daemon            INFO       INFO       INFO
daemon_unix       INFO       INFO       INFO
dpif              INFO       INFO       INFO
dpif_linux        INFO       INFO       INFO
dpif_netdev       INFO       INFO       INFO
dpif_pica         INFO       INFO       INFO
entropy           INFO       INFO       INFO
fail_open         INFO       INFO       INFO
fatal_signal      INFO       INFO       INFO
hmap              INFO       INFO       INFO
hwlog             INFO       INFO       INFO
in_band           INFO       INFO       INFO
inband_bridge     INFO       INFO       INFO
ipfix             INFO       INFO       INFO
jsonrpc           INFO       INFO       INFO
lacp              INFO       INFO       INFO
lcmgr             INFO       INFO       INFO
lcmgr_shared      INFO       INFO       INFO
lldp              INFO       INFO       INFO
lockfile          INFO       INFO       INFO
memory            INFO       INFO       INFO
meta_flow         INFO       INFO       INFO
multipath         INFO       INFO       INFO
netdev            INFO       INFO       INFO
netdev_dummy      INFO       INFO       INFO
netdev_linux      INFO       INFO       INFO
netdev_pica       INFO       INFO       INFO
netdev_pica_lag   INFO       INFO       INFO
netdev_pica_vport  INFO       INFO       INFO
netdev_vport      INFO       INFO       INFO
netflow           INFO       INFO       INFO
netlink           INFO       INFO       INFO
netlink_notifier  INFO       INFO       INFO
netlink_socket    INFO       INFO       INFO
nx_match          INFO       INFO       INFO
```

```
odp_util          INFO       INFO       INFO
ofp_actions       INFO       INFO       INFO
ofp_errors        INFO       INFO       INFO
ofp_msgs          INFO       INFO       INFO
ofp_util          INFO       INFO       INFO
ofproto           INFO       INFO       INFO
ofproto_dpif      INFO       INFO       INFO
ofproto_dpif_mirror  INFO       INFO       INFO
ofproto_dpif_monitor  INFO       INFO       INFO
ofproto_dpif_upcall  INFO       INFO       INFO
ofproto_dpif_xlate  INFO       INFO       INFO
ovs_rcu           INFO       INFO       INFO
ovs_thread        INFO       INFO       INFO
ovsdb_error       INFO       INFO       INFO
ovsdb_idl         INFO       INFO       INFO
pcap              INFO       INFO       INFO
pica_private      INFO       INFO       INFO
pktbuf            INFO       INFO       INFO
poll_loop         INFO       INFO       INFO
process           INFO       INFO       INFO
rconn             INFO       INFO       INFO
reconnect         INFO       INFO       INFO
route_table       INFO       INFO       INFO
sflow             INFO       INFO       INFO
signals           INFO       INFO       INFO
socket_util       INFO       INFO       INFO
stp               INFO       INFO       INFO
stream            INFO       INFO       INFO
stream_fd         INFO       INFO       INFO
stream_ssl        INFO       INFO       INFO
stream_tcp        INFO       INFO       INFO
stream_unix       INFO       INFO       INFO
svec              INFO       INFO       INFO
system_stats      INFO       INFO       INFO
timeval           INFO       INFO       INFO
tunnel            INFO       INFO       INFO
unixctl           INFO       INFO       INFO
user_config       INFO       INFO       INFO
util              INFO       INFO       INFO
vconn             INFO       INFO       INFO
vconn_stream      INFO       INFO       INFO
vlandev           INFO       INFO       INFO
vlog              INFO       INFO       INFO
vswitchd          INFO       INFO       INFO
xenserver         INFO       INFO       INFO
```

ovs-appctl vlog/set

To enable Open vSwitch logging and customize the logging levels, use the **ovs-appctl vlog/set** command.

Syntax

ovs-appctl vlog/set *module*[**:***facility*[**:***level*]]

Parameters

Parameters	
module	A valid module name, as displayed by the ovs-appctl vlog/list command. The log level change is only applied to the specified module. If *module* is not specified, the new settings are applied to all modules.
facility	The log level change is limited to the specified facility. Valid options are **syslog**, **console**, and **file**.
level	Messages of the given severity or higher will be logged, and messages of lower severity will be filtered out. Valid options are **off**, **emer**, **err**, **warn**, **info**, or **dbg**. **off** filters out all messages. If *level* is not specified, the logging level is set to **dbg** (debugging).

Examples

The following example configures debugging messages for Open vSwitch daemon to be logged to the console:

```
admin@Switch$ovs-appctl vlog/set vswitchd:console:dbg
```

Pica8 Commands

Command List

ovs-appctl pica/show

This command displays available resources for open flow.

```
Max Hardware Flow Entry Limitation:
    TCAM Table    : 8192
    Egress Table  : 512
    VFilter Table : 512
    L2 Table      : 32768
    L3 Table      : 24000

Valid Interfaces On Switch as5812_54x:
    Physical interfaces:
        te-1/1/1(1)       te-1/1/2(2)       te-1/1/3(3)       te-1/1/4(4)
        te-1/1/5(5)       te-1/1/6(6)       te-1/1/7(7)       te-1/1/8(8)
        te-1/1/9(9)       te-1/1/10(10)     te-1/1/11(11)     te-1/1/12(12)
        te-1/1/13(13)     te-1/1/14(14)     te-1/1/15(15)     te-1/1/16(16)
        te-1/1/17(17)     te-1/1/18(18)     te-1/1/19(19)     te-1/1/20(20)
        te-1/1/21(21)     te-1/1/22(22)     te-1/1/23(23)     te-1/1/24(24)
        te-1/1/25(25)     te-1/1/26(26)     te-1/1/27(27)     te-1/1/28(28)
        te-1/1/29(29)     te-1/1/30(30)     te-1/1/31(31)     te-1/1/32(32)
        te-1/1/33(33)     te-1/1/34(34)     te-1/1/35(35)     te-1/1/36(36)
        te-1/1/37(37)     te-1/1/38(38)     te-1/1/39(39)     te-1/1/40(40)
        te-1/1/41(41)     te-1/1/42(42)     te-1/1/43(43)     te-1/1/44(44)
        te-1/1/45(45)     te-1/1/46(46)     te-1/1/47(47)     te-1/1/48(48)
        xe-1/1/1(73)      xe-1/1/2(74)      xe-1/1/3(75)      xe-1/1/4(76)
        xe-1/1/5(77)      xe-1/1/6(78)
    LAG   interfaces:    ae1(1025) - ae1023(2047)
    Bond  interfaces:  bond1(2049) - bond1023(3071)
    GRE   interfaces:   gre1(3073) - gre1023(4095)
    VXLAN interfaces: vxlan1(4097) - vxlan1023(5119)
    L2GRE interfaces: l2gre1(5121) - l2gre1023(6143)
```

ovs-appctl bridge/clear-counts bridge *[interface]*

This command clears ports statistics.

```
admin@PicOS-OVS$ovs-appctl bridge/clear-counts br0
admin@PicOS-OVS$ovs-appctl bridge/clear-counts br0 ge-1/1/1
```

ovs-appctl pica/dump-flows [--sort | --rsort]

Shows the hardware flow.

User can use [--sort|--rsort]to sort the output of the hardware flow dump by priority.

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
Total 3 flows in HW.

admin@PicOS-OVS$ovs-appctl pica/dump-flows --sort
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
Total 3 flows in HW.
```

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows --rsort
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#0 normal_d permanent flow_id=2 priority=0, actions:drop
Total 3 flows in HW.
```

ovs-appctl bridge/dump-flows bridge

Shows all software flows, including those flows not added by user or switch.

```
admin@SpineA-OVS$ovs-appctl bridge/dump-flows br0
duration=2402s, n_packets=n/a, n_bytes=0, priority=24600,dl_vlan=4094,dl_dst=02:00:00:08:00:01/ff:03:ff:ff:ff:ff,a
duration=2402s, n_packets=n/a, n_bytes=0, priority=24600,dl_vlan=4094,dl_dst=02:00:00:08:00:02/ff:03:ff:ff:ff:ff,a
duration=2656s, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,nw
duration=2656s, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,nw
duration=2658s, n_packets=n/a, n_bytes=38984, priority=65535,dl_type=0x88cc,actions=CONTROLLER:65535
duration=2656s, n_packets=n/a, n_bytes=0, priority=22000,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,acti
duration=2656s, n_packets=n/a, n_bytes=0, priority=22000,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,acti
duration=2656s, n_packets=n/a, n_bytes=23628, priority=2,in_port=1,actions=CONTROLLER:65535
duration=2656s, n_packets=n/a, n_bytes=15710, priority=2,in_port=2,actions=CONTROLLER:65535
duration=53s, n_packets=n/a, n_bytes=1152296, priority=25000,in_port=1,dl_vlan=100,dl_src=00:0c:29:fd:75:ae,dl_dst=
duration=48s, n_packets=n/a, n_bytes=1588, priority=25000,in_port=2,dl_vlan=100,dl_src=00:0c:29:70:2e:b8,dl_dst=00
duration=2658s, n_packets=n/a, n_bytes=0, priority=0,actions=drop
duration=2656s, n_packets=n/a, n_bytes=576, priority=22016,arp,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:0
duration=2656s, n_packets=n/a, n_bytes=1220, priority=22016,arp,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:
duration=2656s, n_packets=n/a, n_bytes=512, priority=22016,rarp,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:
duration=2656s, n_packets=n/a, n_bytes=512, priority=22016,rarp,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=1,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x3,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x1,actions=controller(reason=no_match)
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x2,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=2,recirc_id=0,actions=resubmit(,0)
```

ovs-appctl cfm/set-fault *[interface]* normal|false|true

If true, a CFM fault was manually triggered.
If false, force to set no CFM fault.
If normal, return to normal CFM.

ovs-appctl cfm/show *[interface]*

Show cfm status.

```
admin@PicOS-OVS$ovs-appctl cfm/show
---- te-1/1/49 ----
MPID 2000: extended fault_override
fault: override
average health: 100
opstate: up
remote_opstate: up
interval: 1000ms
next CCM tx: 879ms
next fault check: 165ms
Remote MPID 2100
recv since check: true
opstate: up
---- te-1/1/50 ----
MPID 2001: extended fault_override
fault: override
average health: 100
opstate: up
remote_opstate: up
interval: 1000ms
next CCM tx: 879ms
next fault check: 569ms
Remote MPID 2101
recv since check: true
```

```
opstate: up
```

ovs-appctl inband/dump-flows bridge

Show inband flows.

ovs-appctl inband/enable true|false

Enable or disable inband mode.

ovs-appctl inband/show

Show inband status.

ovs-appctl lacp/show

This command displays the LACP status on the configured ports.

```
admin@PicOS-OVS$ovs-appctl lacp/show
---- ae1 ----

status: active negotiated
sys_id:00:11:11:11:11:11
sys_priority: 32768
aggregation key: 1
lacp_time: fast

slave: ge-1/1/1:
current attached
port_id: 1
port_priority: 32768
may_enable: true
actor sys_id:00:11:11:11:11:11
actor sys_priority:32768
actor port_id: 1
actor port_priority:32768
actor key: 1
actor state: activity timeout synchronized collecting distributing
partner sys_id:00:0c:29:fd:75:b8
partner sys_priority: 65535
partner port_id: 2
partner port_priority:255
partner key: 17
partner state: activity timeout aggregation synchronized collecting distributing
---- ae2 ----
status: passive
sys_id: ff:ff:ff:ff:ff:00
sys_priority: 32768
aggregation key: 3
lacp_time: slow

slave: te-1/1/3: current detached
port_id: 3
port_priority: 32768
may_enable: false

actor sys_id: ff:ff:ff:ff:ff:00
actor sys_priority: 32768
actor port_id: 3
actor port_priority: 32768
actor key: 3
actor state: collecting distributing

partner sys_id: ff:ff:ff:ff:ff:00
partner sys_priority: 32768
partner port_id: 2
partner port_priority: 32768
partner key: 2
partner state: activity collecting distributing
```

ovs-appctl Target Commands

This section includes one command of target. ovs-appctl -t <target> <command> The default <target> is ovs-vswitchd.

- ovs-appctl -t ovs-vswitchd <command>

ovs-appctl -t ovs-vswitchd <command>

ovs-appctl -t ovs-vswitchd lacp/show

Display the information of LACP.

ovs-appctl -t ovs-vswitchd dpif/dump-flows <bridge>

This command can be used in OVS 2.0.

ovs-appctl -t ovs-vswitchd bridge/dump-flows <bridge>

ovs-appctl -t ovs-vswitchd pica/dump-flows

This command can be used in OVS 2.0. Using this command user can print hardware flows..

ovs−ofctl Commands

ovs−ofctl is a utility for managing OpenFlow switches. **ovs-ofctl** should work with any OpenFlow switch, not just Open vSwitch.

Users can view the **ovs-ofctl** help for more information about the utility.

```
admin@Leaf1$ovs-ofctl --help
ovs-ofctl: OpenFlow switch management utility
usage: ovs-ofctl [OPTIONS] COMMAND [ARG...]
For OpenFlow switches:
  show SWITCH                 show OpenFlow information
  dump-desc SWITCH            print switch description
  dump-tables SWITCH          print table stats
  dump-table-features SWITCH  print table features
  mod-port SWITCH IFACE ACT   modify port behavior
  mod-table SWITCH MOD        modify flow table behavior
  get-frags SWITCH            print fragment handling behavior
  set-frags SWITCH FRAG_MODE  set fragment handling behavior
  dump-ports SWITCH [PORT]    print port statistics
  dump-ports-desc SWITCH [PORT]  print port descriptions
  dump-flows SWITCH           print all flow entries
  dump-flows SWITCH FLOW      print matching FLOWs
  dump-aggregate SWITCH       print aggregate flow statistics
  dump-aggregate SWITCH FLOW  print aggregate stats for FLOWs
  queue-stats SWITCH [PORT [QUEUE]]  dump queue stats
  add-flow SWITCH FLOW        add flow described by FLOW
  add-flows SWITCH FILE       add flows from FILE
  mod-flows SWITCH FLOW       modify actions of matching FLOWs
  del-flows SWITCH [FLOW]     delete matching FLOWs
  replace-flows SWITCH FILE   replace flows with those in FILE
  diff-flows SOURCE1 SOURCE2  compare flows from two sources
  packet-out SWITCH IN_PORT ACTIONS PACKET...
                              execute ACTIONS on PACKET
  monitor SWITCH [MISSLEN] [invalid_ttl] [watch:[...]]
                              print packets received from SWITCH
  snoop SWITCH                snoop on SWITCH and its controller
  add-group SWITCH GROUP      add group described by GROUP
  add-groups SWITCH FILE       add group from FILE
  mod-group SWITCH GROUP      modify specific group
  del-groups SWITCH [GROUP]   delete matching GROUPs
  dump-group-features SWITCH  print group features
  dump-groups SWITCH [GROUP]  print group description
  dump-group-stats SWITCH [GROUP]  print group statistics
  queue-get-config SWITCH PORT  print queue information for port
  add-meter SWITCH METER      add meter described by METER
  mod-meter SWITCH METER      modify specific METER
  del-meter SWITCH METER      delete METER
  del-meters SWITCH           delete all meters
  dump-meter SWITCH METER     print METER configuration
  dump-meters SWITCH          print all meter configuration
  meter-stats SWITCH [METER]  print meter statistics
  meter-features SWITCH       print meter features
For OpenFlow switches and controllers:
  probe TARGET                probe whether TARGET is up
  ping TARGET [N]             latency of N-byte echos
  benchmark TARGET N COUNT    bandwidth of COUNT N-byte echos
SWITCH or TARGET is an active OpenFlow connection method.
Other commands:
  ofp-parse FILE              print messages read from FILE
  mod-temp-thresh SWITCH THRESHOLD  modify temperature threshold
  dump-temp-thresh SWITCH     print temperature threshold
  ofp-parse-pcap PCAP         print OpenFlow read from PCAP
  dump-tables-desc SWITCH     print tables description
  bundle SWITCH MSG           send bundle messages
Active OpenFlow connection methods:
  tcp:IP[:PORT]           PORT (default: 6633) at remote IP
  ssl:IP[:PORT]           SSL PORT (default: 6633) at remote IP
```

```
  unix:FILE               Unix domain socket named FILE
PKI configuration (required to use SSL):
  -p, --private-key=FILE  file with private key
  -c, --certificate=FILE  file with certificate for private key
  -C, --ca-cert=FILE      file with peer CA certificate
Daemon options:
  --detach                run in background as daemon
  --no-chdir              do not chdir to '/'
  --pidfile[=FILE]        create pidfile (default: /ovs/var/run/openvswitch/ovs-ofctl.pid)
  --overwrite-pidfile     with --pidfile, start even if already running
OpenFlow version options:
  -V, --version           display version information
  -O, --protocols         set allowed OpenFlow versions
                          (default: OpenFlow10, OpenFlow11, OpenFlow12, OpenFlow13, OpenFlow14)
Logging options:
  -vSPEC, --verbose=SPEC   set logging levels
  -v, --verbose            set maximum verbosity level
  --log-file[=FILE]        enable logging to specified FILE
                           (default: /ovs/var/log/openvswitch/ovs-ofctl.log)
  --syslog-target=HOST:PORT  also send syslog msgs to HOST:PORT via UDP
Other options:
  --strict                    use strict match for flow commands
  --readd                     replace flows that haven't changed
  -F, --flow-format=FORMAT    force particular flow format
  -P, --packet-in-format=FRMT force particular packet in format
  -m, --more                  be more verbose printing OpenFlow
  --timestamp                 (monitor, snoop) print timestamps
  -t, --timeout=SECS          give up after SECS seconds
  --sort[=field]              sort in ascending order
  --rsort[=field]             sort in descending order
  --unixctl=SOCKET            set control socket name
  -h, --help                  display this help message
  -V, --version               display version information
```

See ovs-ofctl manual page for detailed syntax and additional information.

```
admin@Leaf1$man ovs-ofctl
ovs-ofctl(8)                                    Open vSwitch Manual                                    ovs-of
NAME
       ovs-ofctl - administer OpenFlow switches
SYNOPSIS
       ovs-ofctl [options] command [switch] [args...]
DESCRIPTION
       The ovs-ofctl program is a command line tool for monitoring and administering OpenFlow switches.  It can als
       the current state of an OpenFlow switch, including features, configuration, and table  entries.   It  should
       with any OpenFlow switch, not just Open vSwitch.
   OpenFlow Switch Management Commands
       These commands allow ovs-ofctl to monitor and administer an OpenFlow switch.  It is able to show the current
       of a switch, including features, configuration, and table entries
<Some output omitted>
```

ovs-ofctl Common Commands

- ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl dump-desc <bridge>
- ovs-ofctl del-group <bridge> [group_id=<id>]
- ovs-ofctl mod-table <bridge> <table> <mod>
- ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]
- ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl dump-tables <bridge>
- ovs-ofctl dump-tables-desc <bridge>
- ovs-ofctl mod-flows <bridge> <flow>
- ovs-ofctl add-flow <bridge> <flow>
- ovs-ofctl del-meters <bridge>
- ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl add-flows <bridge> <file>
- ovs-ofctl del-meter <bridge> meter=<id>
- ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl show <bridge>
- ovs-ofctl dump-ports-desc <bridge>
- ovs-ofctl bundle <bridge> <bundle>

- ovs-ofctl dump-flows <bridge> <flow>
- ovs-ofctl snoop <bridge>
- ovs-ofctl dump-ports <bridge> <port>
- ovs-ofctl del-flows <bridge> <flow>
- ovs-ofctl mod−port <bridge> <iface> <action>
- ovs-ofctl replace-flows <bridge> <file>
- ovs-ofctl diff-flows <source1> <source2>
- ovs-ofctl add-groups <bridge> <file>
- ovs-ofctl queue-get-config <bridge> <port>
- ovs-ofctl meter-stats <bridge> [meter]
- ovs-ofctl meter-features <bridge>

ovs-ofctl dump-meters <bridge>

---

ovs-ofctl Common Commands

Most of these commands take an argument that specifies the method for connecting to an OpenFlow switch. The following connection methods are supported:

- ovs-ofctl add-flow <bridge> <flow>
- ovs-ofctl add-flows <bridge> <file>
- ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl bundle <bridge> <bundle>
- ovs-ofctl del-flows <bridge> <flow>
- ovs-ofctl del-group <bridge> [group_id=<id>]
- ovs-ofctl del-meter <bridge> meter=<id>
- ovs-ofctl del-meters <bridge>
- ovs-ofctl dump-desc <bridge>
- ovs-ofctl dump-flows <bridge> <flow>
- ovs-ofctl dump-ports <bridge> <port>
- ovs-ofctl dump-ports-desc <bridge>
- ovs-ofctl dump-tables <bridge>
- ovs-ofctl dump-tables-desc <bridge>
- ovs-ofctl mod-flows <bridge> <flow>
- ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl mod-table <bridge> <table> <mod>
- ovs-ofctl mod−port <bridge> <iface> <action>
- ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]
- ovs-ofctl show <bridge>
- ovs-ofctl snoop <bridge>
- ovs-ofctl replace-flows <bridge> <file>
- ovs-ofctl diff-flows <source1> <source2>
- ovs-ofctl add-groups <bridge> <file>
- ovs-ofctl queue-get-config <bridge> <port>
- ovs-ofctl meter-stats <bridge> [meter]
- ovs-ofctl meter-features <bridge>

ovs-ofctl add-flow <bridge> <flow>

Add flow described by flow.

ovs-ofctl add-flow <bridge> in_port=<port>,actions=<action>

Matches the in_port port in open flow, <port> can be a port number or keyword (eg:LOCAL).

ovs-ofctl add-flow <bridge> dl_vlan=<vlanid>,actions=<action>

Add a flow with the match field dl_vlan (IEEE 802.1q Virtual LAN tag). When the VLAN ID of the packets matches the flow match field then it will be forward according to the actions.The VLAN value ranges from 0 to 4095.

ovs-ofctl add-flow <bridge> dl_vlan_pcp=<value>,actions=<action>

dl_vlan_pcp is an identifier that matches IEEE 802.1q Priority Code Point (PCP) priority. It is a value between 0 and 7. When the value is higher, frame priority level is higher.

ovs-ofctl add-flow <bridge> dl_src=<mac>,actions=<action>

Add a flow with the match field dl_src that matches an Ethernet source address. This value uses 6 pairs of hexadecimal digits to specify, eg: 00:0B:C4:A8:22:B0.

ovs-ofctl add-flow <bridge> dl_dst=<mac>,actions=<action>

Add a flow with the match field dl_dst that matches an Ethernet destination address. This value uses 6 pairs of hexadecimal digits to specify, eg: 00:0B:C4:A8:22:B0.

ovs-ofctl add-flow <bridge> dl_src=<mac/mask>,actions=<action>

ovs-ofctl add-flow <bridge> dl_dst=<mac/mask>,actions=<action>

This type of source mac address provides a wider match field. When the 6 pairs of masks are full *ff*, it indicates exact match, as to say, it is the same with *dl_src=xx:xx:xx:xx:xx:xx.* Otherwise,1-bit in mask indicates that the corresponding bit in *mac* must match exactly, 0-bit in mask indicates wildcards.

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,actions=<action>

Matches Ethernet protocol type *ethertype*, which is specified as an integer between 0 and 65535, inclusive, either in decimal or as a hexadecimal number prefixed by **0x.** (e.g. **0x0806** to match ARP packet).

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_src=ip[/netmask],actions=<action>

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_dst=ip[/netmask],actions=<action>

nw_src and nw_dst are the identifiers of IP source/destination addresses. But before the IP source/destination address is set, Ethernet Type(dl_type) must be set.Type values include：0x0800: matches IPv4 source/destination address IP (eg:ip, tcp). 0x0806: the arp protocol type, matches the ar_sqa or ar_tpa field. respectively, in ARP packets for IPv4 and Ethernet. 0x8035:therarp protocol type, matches the ar_spa or ar_tpa field, respectively, in RARP packets for IPv4 and Ethernet. Other than 0x0800, 0x0806, or 0x8035, the values of nw_src and nw_dst are ignored

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_proto=<proto>, actions=<action>

This parameter <proto> is specified as a decimal number with the value between 0-255.
When dl_type=0x86dd or IPv6 is specified, the packets must match IPv6 header type.Set proto to 58 to match ICMPv6 packets.
When dl_type=0x0806 or arp is specified,packets must match the lower 8 bits of the ARP opcodes. The opcodes greater than 255 are treated as 0.
When dl_type=0x8035 or rarp is specified,packets must match the lower 8 bits of the RARP opcodes The opcodes greater than 255 are treated as 0.

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_tos=<tos>, actions=<action>

This parameter <tos> is specified as a decimal number with the value between 0-255. When dl_type=0x0800 or 0x86dd is specified,matches the IP TOS/DHCP or IPv6 traffic class field tos. Note that the two lower reserved bits of tos are ignored for matching purposes. When **dl_type** is wildcarded or set to a value other than 0x0800 or 0x86dd, the value of **nw_tos** is ignored (see **Flow Syntax** above).

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_ecn=<ecn>,actions=<action>

This parameter <tos> is specified as a decimal number with the value between 0-3. When dl_type=0x0800 or 0x86dd is specified,matches the *ecn* bits in IP ToS or IPv6 traffic class fields .When **dl_type** is wildcarded or set to a value other than 0x0800 or 0x86dd, the value of **nw_ecn** is ignored

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_src=<port>,actions=<action>

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port>,actions=<action>

When you want to match **tp_src** or **tp_dst**, you must specify**dl_type** and **nw_proto**as TCP or UDP , <port> is specified as decimal number between 0-65535. When **dl_type** and **nw_proto** take other values, the values of these settings are ignored.

ovs-ofctl add-flow <bridge> dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port/mask>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port/mask>,actions=<action>

When you set the **tp_src** and **tp_dst** like this, that means bitwise match on TCP (or UDP) source or destination port. Both the port and mask are 16-bit decimal numbers or hexadecimal numbers prefixed by 0X. Each 1bit in mask requires the corresponding bit in port must match, while each 0-bit in mask requires the corresponding bit in port to be ignored.

ovs-ofctl add-flow <bridge> table=<number><flow>

By default, the table number is 0. When **table** number is specified, that will limit flow manipulations and dump flow commands to apply to the specified table number which is between 0-254.

ovs-ofctl add-flow <bridge> metadata=value[/mask]<flow>

metadata is just useful across multiple flow tables. It makes matching flows easy. Sometimes, we will just check the **metadata** of flow because different metadata means different flows. But this field is only applied to software flow tables, not applied to the only hardware flow table in our switch.

ovs-ofctl add-flow<bridge> dl_type=<ethernettype>,nw_proto=1,icmp_type=<type>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=<ethernettype>,nw_proto=1,icmp_code=<type>,actions=<action>

When you specify **dl_type** and**nw_proto** as ICMP or ICMPv6,then **icmp_type** must matches the ICMP type (eg:**icmp_type=1**), and **icmp_code** must matched ICMP code that the value of code is between 0-255.
When **dl_type** and **nw_proto** take other values, the values of these settings are ignored.

ovs-ofctl add-flow<bridge> dl_type=0x8847,mpls_label=<label>,actions=<action>

The value of mpls label is between 0-1048575.That is to say you can add 1048575 mpls labels at most.

ovs-ofctl add-flow<bridge> dl_type=0x8847,mpls_tc=<tc>,actions=<action>

The value of **mpls_tc** is between 0-7.It is for experimental use.

ovs-ofctl add-flow<bridge> vlan_tci=<tci[/mask]>,actions=<action>

The tci matches VLAN TCI. The tci and mask are 16-bit values are decimal by default;you can use a 0x prefix to set the values in hexadecimal.when mask is specified,1-bit number in mask requires corresponding bit in tci must match exact,and 0-bit in mask makes corresponding bit in tci be ignored.If do not specify mask,thentci is the exact VLAN TCI to match.

ovs-ofctl add-flow<bridge> dl_type=0x86DD,ipv6_src=<ipv6[/netmask]>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=0x86DD,ipv6_dst=<ipv6[/netmask]>,actions=<action>

If you want to add a flow with the ipv6 source and destination,you must first set the dl_type as 0x86dd(or ipv6 or tcp6).
The actions of flow include the following values,all the values are applied into add-flow, add-flows, and mod-flows .These are just examples of add-flow below.

ovs-ofctl add-flow<bridge><match-field>actions=[target][,target...]

ovs-ofctl add-flow<bridge><match-field>actions=output:<port>

The port should be an OpenFlow port number or keyword as LOCAL and so on.That means outputting packets to port.

ovs-ofctl add-flow<bridge><match-field>actions=enqueue:<port>:<queue>

The *port* should be an OpenFlow port number or keyword(eg:LOCAL).This action means to enqueue the packets on specified *queue* within the port.The queues numbers depend on switch.

ovs-ofctl add-flow<bridge><match-field>actions=NORMAL

This action means making packets be processed as device' normal L2/L3.

ovs-ofctl add-flow<bridge><match-field>actions=flood

This action means outputting packets on all physical ports other than the port on which it was receivedand any ports on which flooding is disabled (typically, these would be ports disabled by the IEEE 802.1D spanning tree protocol).

ovs-ofctl add-flow <bridge> <match-field> actions=all

This action means outputting packets on all physical ports other than the port on which it was received.

ovs-ofctl add-flow <bridge> <match-field>actions=controller(key=value...)

When you set action as controller, the packets will be sent in OpenFlow controller as packet-in message.

ovs-ofctl add-flow <bridge> <match-field>actions=drop

This action means discard the packets without further processing or forwarding. When this action **drop** is used,you should not specify other actions.

ovs-ofctl add-flow <bridge> <match-field> actions=push_vlan:<ethertype>,set_field:<value>-\>vlan_vid,output:<port>

Using **push_vlan**, you can push a new VLAN to packets, *ethertype* is the ethertype for the tag **(**only support **0x8100** at the moment. **set_field** is used to set the value of priority.

ovs-ofctl add-flow <bridge> <match-field> dl_type=<ethertype>,dl_src=<src>,dl_dst=<dst>,actions=push_mpls:<ethertype>,set_field:<value>-\>mpls_label,output:<port>

Using **push_mpls,** you can push a new mpls label for a packet without any mpls label. At this time,the *ethertype* must be either MPLS unicast ethertype**0x8847,** or the MPLS multicast ethertype**0x8848.** if the packets has already contains a mpls label, pushes a new outermost label as a copy of the existing outermost label.

ovs-ofctl add-flow<bridge><match-field>actions=pop_mpls:<ethertype>

You can pop outer mpls label by setting *ethertype*to MPLS Ethertype.and pop all MPLS label by setting *ethertype* to the types except mplsethertype.

ovs-ofctl add-flow<bridge><match-field>actions=push_pbb:<ethertype>,set_field:<value>-\...

You can push outermost mac address for packets.PBB is a mac-in-mac technology.ethertype is **0x88e7.**

ovs-ofctl add-flow<bridge><match-field>actions=pop_pbb

You can pop the outer mac for packets by using pop_pbb.

ovs-ofctl add-flow<bridge><match-field>actions=mod_vlan_vid:<vlan_vid>

This action means modify the thevlan id of the packets.Thevlan tag is added or modified as necessary to match specifiedvalue.when the vlan tag is added ,then priority of the packets are 0 by default.You can set priority by **mod_vlan_pcp**.*vlan_id* is between 0-4095.

ovs-ofctl add-flow<bridge><match-field>actions=mod_vlan_pcp:<vlan_pcp>

You can modify the vlan priority of the packets.vlan_pcp value is between0-7, 0 presents the lowest priority and 7 means highest priority.

ovs-ofctl add-flow<bridge><match-field>actions=strip_vlan

Using this action ,you can pop vlan tag from packets.

ovs-ofctl add-flow<bridge><match-field>actions=mod_dl_src:<mac>

User can modify source mac of packets from the output port by **mod_dl_src.**

ovs-ofctl add-flow<bridge><match-field>actions=mod_dl_dst:<mac>

User can modify *destination* mac of packets from the output port by **mod_dl_dst**

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_src:<ip>

Modify the *source ipv4* addressof specified flow,by using mod_nw_src.

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_dst:<ip>

Modify the *destination ipv4* addressof specified flow,by using mod_nw_dst.

ovs-ofctl add-flow<bridge><match-field>actions=mod_tp_src:<port>

Modify the TCP or UDP source port.

ovs-ofctl add-flow<bridge><match-field>actions=mod_tp_dst:<port>

Modify the TCP or UDP destination port.

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_tos:<tos>

By using this action you can modify the IPv4 TOS or DSCP field to tos, which must be a multiple of 4 between 0-255.This action can not modify the lower 2-bits of tos field which represents ECN bits.

ovs-ofctl add-flow<bridge><match-field>actions=resubmit([port],[table])

By this action,you can re-search OpenFlow flow table with the**in_port** field replaced by *port*. Or research the table whose number is specified by table.

ovs-ofctl add-flow<bridge><match-field>actions=set_queue:<queue>

By taking this action, the packets that is output the port will be output the specified *queue*. Different switch has different numbers of supported queues.

ovs-ofctl add-flow<bridge><match-field>actions=set_mpls_ttl:ttl

This action will set the TTL of outer MPLS label stack entry of a packet. The range of TTL number is between 0-255.

ovs-ofctl add-flow<bridge><match-field>actions=controller(key=value...)

Taking this action will send packets to OpenFlow controller as "packet-in" message. There are some key-value pairs as follow.
max_len=*nbytes:* limit the maximum length of packets sent to the controller. By default, the entire packet is sent.
reason=*reason:*Specify *reason* as the reason for sending the message in the ''packet in'' message. The supported reasons are **action** (the default), **no_match**, and **invalid_ttl**.

ovs-ofctl add-flow <bridge> in_port=<port>,ip, actions=set_field:16-\>tos,output:<port>

modify the value of tos in packets.

support vntag and vnid in match fields now.

ovs-ofctl add-flow <bridge> vn_tag=0x33330000/0x3FFF0000,dl_dst=00:11:11:11:11:11,actions=2. For the details,check the link:VN-tag.

ovs-ofctl add-flow <bridge> **udp,tp_dst=5000,tun_id=0x0200000000112233,actions=2**

support the udf fields

ovs-ofctl add-flow <bridge> table=250,in_port=<port>,udf0=0x810003E8/0x0000ffff,actions=2

please check the details through the following link:Configuring udf flow

Summarize Above Flows as a Table

ovs-ofctl add-flow <bridge> <flow>

Add table:

feature	Match fields	actions	example
L2	in_port=<port>	<action>	ovs-ofctl add-flow br0 in_port=1,actions=output:2
	dl_src=<mac>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_src=22:22:22:22:22:22,actions=output:2
	dl_dst=<mac>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_dst=00:0B:C4:A8:22:B0,actions=output:2
	dl_src=<mac/mask>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_src=00:0B:C4:A8:22:B0/ff:ff:ff:ff:ff:ff,actions=output:2
	dl_dst=<mac/mask>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_dst=00:0B:C4:A8:22:B0/ff:ff:ff:ff:ff:ff,actions=output:2
	dl_type=<ethernet type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=output:2
	<match-field>	mod_dl_src:<mac> /set_field:22:22:22:22:33:33-\>dl_dst	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_dst=22:22:22:22:22:22,actions=mod_dl_src:22:23:33:33:33:33,output:2
	<match-field>	mod_dl_dst:<mac> /set_field:22:22:22:22:44:44-\>dl_src	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=mod_dl_dst:22:23:33:33:33:33,output:2
L3	dl_type=<ethernet type>,nw_src=ip[/netmask]	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=1.1.1.0/24,actions=output:2
	dl_type=<ethernet type>,nw_dst=ip[/netmask]	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_dst=1.1.1.0/24,actions=output:2
	dl_type=<Ethernet type>, nw_proto=<proto>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,nw_proto=17,actions=set_field:22:33:33:33:33:33-\>dst,output:2
	dl_type=<ethernet type>, nw_ecn=<ecn>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,nw_ecn=1,actions= output:2
	dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_src=800,actions= output:2
	dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_dst=800,actions= output:2
	dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port/mask>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_src= 2002/oxffff,actions= output:2
	dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port/mask>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_dst=2002/oxffff,actions= output:2
	<match-field>	mod_nw_src:<ip> /set_field:2.2.2.2-\>nw_src	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,actions=mod_nw_src:1.1.1.1,output=2
	<match-field>	mod_nw_dst:<ip> /set_field:3.2.2.3-\>nw_dst	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,actions=mod_nw_src:1.1.1.1,output=2
	<match-field>	tcp: mod_tp_src:<port> /set_field:800-\>tp_src udp: set_field:800-\>udp_src	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,tcp,actions=mod_tp_src:2002,output=2 ovs-ofctl add-flow br0 in_port=1,udp,nw_src=1.1.1.1,actions=set_field:800-\>udp_src,output=2
	<match-field>	tcp: mod_tp_dst:<port> /set_field:900-\>tp_dst udp: set_field:800-\>udp_dst	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,tcp,actions=mod_tp_dst:2002,output=2 ovs-ofctl add-flow br0 in_port=1,udp,nw_dst=1.1.1.1,actions=set_field:880-\>udp_dst,output=2
Table	table=<number>	<action>	ovs-ofctl add-flow br0 in_port=1,ip,table=251,dl_dst=22:22:22:22:22:22,actions=push_vlan:0x8100,set_field:1999-\>vlan_vid,output:2
Metadata	metadata=value[/mask]	<action>	
ICMP	dl_type=<ethernettype>,nw_proto=1,icmp_type=<type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_proto=1,icmp_type=0,nw_dst=96.115.0.0/17,actions=meter:2,all
	dl_type=<ethernettype>,nw_proto=1,icmp_code=<type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_proto=1,icmp_type=8,icmp_code=100,actions=output:2"
MPLS	dl_type=0x8847,mpls_label=<label>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,mpls_label=222,actions=push_mpls:0x8847,set_field:30-\>mpls_label,output:2
	dl_type=0x8847,mpls_tc=<tc>	set_field:<value> -\>mpls_tc	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,mpls_tc=1,actions=set_field:2-\>mpls_tc,output:2
	<match-field> dl_type=<ethertype>,dl_src=<src>,dl_dst=<dst>	push_mpls:<ethertype>,set_field:<value>-\>mpls_label,output:<port>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22, actions=push_mpls:0x8847,set_field:222-\>mpls_label,output:2
	<match-field>	pop_mpls:<ethertype>	ovs-ofctl add-flow br0 in_port=5,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,mpls_tc=2,actions=push_mpls:0x8847,set_field:222-\>mpls_label,output:6
	<match-field>	set_mpls_ttl:ttl	ovs-ofctl add-flow br0 in_port=5,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,actions=push_mpls:0x8847,set_field:222->mpls_label,set_mpls_ttl:253,output:6
VLAN	vlan_tci=<tci[/mask]>	<action>	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=6
	dl_vlan=<vlanid>	<action>	ovs-ofctl add-flow br0 in_port=5,dl_vlan=2999,actions=6
	dl_vlan_pcp=<value>	<action>	ovs-ofctl add-flow br0 in_port=5,dl_vlan_pcp=2,actions=output:6
	<match-field>	push_vlan:<ethertype>,set_field:	ovs-ofctl add-flow br0 in_port=1,ip,actions=push_vlan:0x8100,set_field:2999-\>vlan_vid,output:2

		<value>-\>vlan_vid,output:<port>	
	<match-field>	mod_vlan_vid:<vlan_vid> /set_field:299-\>vlan_vid	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=mod_vlan_vid:888,output:6
	<match-field>	mod_vlan_pcp:<vlan_pcp> /set_field:3-\>vlan_pcp	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=mod_vlan_pcp:5,output:6
	<match-field>	strip_vlan	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=strip_vlan,output:6
IPv6	dl_type=0x86DD,ipv6_src=<ipv6[/netmask]>	set_field:2002::1-\>ipv6_src	ovs-ofctl add-flow br0 in_port=1,dl_type=0x86dd,ipv6_src=2001::1/128,actions= set_field:2002::1-\>ipv6_src,output:2
	dl_type=0x86DD,ipv6_dst=<ipv6[/netmask]>	set_field:2002::1-\>ipv6_dst	ovs-ofctl add-flow br0 in_port=1,dl_type=0x86dd,ipv6_dst=2001::1/128,actions= set_field:2002::1-\>ipv6_dst,output:2
Openflow	<match-field>	actions=[target][,target...]	
	<match-field>	actions=output:<port>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_vlan=2999,actions= output:2
	<match-field>	actions=enqueue(port,queue)	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=enqueue\(1,7\)
	<match-field>	NORMAL	ovs-ofctl add-flow br0 in_port=1,dl_vlan=2999,actions=NORMAL
	<match-field>	flood	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=flood
	<match-field>	all	ovs-ofctl add-flow br0 in_port=1,dl_vlan=2999,actions=all,set_field:22:33:33:33:33:33-\>dl_dst,output:2,3
	<match-field>	drop	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=all
	<match-field>	controller(key=value...)	ovs-ofctl add-flow br0 arp,arp_op=1,actions=CONTROLLER
PBB	<match-field>	push_pbb:<ethertype>,set_field:<value>-\>pbb_isid	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22,actions=push_pbb:0x88e7,push_vlan:0x8100,set_field:4094-\>vlan_vid,output:2
	<match-field>	pop_pbb	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8100,dl_src=00:00:00:11:11:11,dl_dst=00:00:00:22:22:22,actions=pop_vlan,pop_pbb,output:2
	<match-field>	resubmit([port],[table])	ovs-ofctl add-flow br0 table=0,dl_dst=00:00:00:00:11:11,actions=resubmit\(6,1\) Note: at least one "in_port" or "table" must be specified on resubmit
Qos	<match-field>	mod_nw_tos:<tos> /set_field:16-\>ip_dscp	ovs-ofctl add-flow br0 table=253,dl_type=0x0800,nw_dst=1.1.1.1,actions=mod_nw_tos:16
	<match-field>	set_queue:<queue>	ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=set_queue:0,output=3
	dl_type=<ethernet type>, nw_tos=<tos>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_tos=16,nw_dst=1.1.1.1,actions=mod_nw_tos:32

ovs-ofctl add-flows <bridge> <file>

Add multiple flows from file. You can create a file with many flows in the server, and copy this file to your switch. Then use this command **ovs-ofctl add-flows <bridge> <file>** to add these flows in this file.

Command

ovs-ofctl add-flows <bridge> <file>

Example

There are two flows in file 111.txt. Add these flows in this file as below:

admin@PicOS-OVS$sudo scp sophia.sun@10.10.50.20:/home/sophia.sun/111.txt ./
The authenticity of host '10.10.50.20 (10.10.50.20)' can't be established.
ECDSA key fingerprint is 8f:f3:ca:a1:b9:a9:67:26:e1:54:dc:6a:62:74:d5:f6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.50.20' (ECDSA) to the list of known hosts.
sophia.sun@10.10.50.20's password:
111.txt 100% 54 0.1KB/s 00:00
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ls
111.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flows br0 111.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=10.804s, table=0, n_packets=n/a, n_bytes=0, in_port=7 actions=output:8
cookie=0x0, duration=10.800s, table=0, n_packets=n/a, n_bytes=0, in_port=8 actions=output:9

ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>

PicOS OVS supports group tables from Openflow 1.2.

ovs-ofctl add-group *<bridge>* group_id=*<id>*,type=all,bucket=*<actions>[,bucket=<actions>]*

Add a group that group_id=<id>, type=all in <bridge>. The max buckets number can be created is 10.

Example:
Create a group type=all, include two buckets to modify the src-mac and dst-mac.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=all,bucket=mod_dl_src=00:00:00:11:11:11,mod_dl_dst=00:00:0
```

ovs-ofctl add-group *<bridge>* group_id=*<id>*,type=indirect,bucket=*<actions>*

Add a group that group_id=<id>, type=indirect in <bridge>.

Example:
Create a group type=indirect, just include one bucket to modify the src-mac and dst-mac.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=mod_dl_src=00:00:00:99:11:11,mod_dl_dst=00
```

ovs-ofctl add-group *<bridge>* group_id=*<id>*,type=select,bucket=*<actions>[,bucket=<actions>]*

Add a group that group_id=<id>, type=select in <bridge>.
PisOS OVS is not support weighting now, user cannot specify the weight, weight=1.
Because OVS forwards packets by TCAM, the traditional ECMP in the routing table can not be used in OVS mode.
We implement a "dummy ECMP" by splitting the matching fields of a flow. By the group that type=select, the system will choose one match field to split in nw_src, nw_dst, dl_src, dl_dst. The nw_src is the highest priority, if it has no special nw_src or if the mask of nw_src is 32, it will choose nw_dst. The last choose dl_src and dl_dst. The premise is the match fields must have mask except 32 nor ff:ff:ff:ff:ff:ff.
Exception to this use, is other flows involved with the select group will be packet-driven flows.
Example:
Create a group type=select, the actions of multi buckets only have output.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=3,type=select,bucket=bucket=output:1,output:2,bucket=output:3,bucl
```

ovs-ofctl add-group *<bridge>* group_id=*<id>*,type=ff,bucket=*<actions>[,bucket=<actions>]*

Add a group that group_id=<id>, type=ff, in <bridge>. The ff means fast_failover.
Example:

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=4,type=ff,bucket=watch_port:2,watch_group:2,output:3,watch_port:3
```

Actions supported table:

Chip	Firebolt3								Triumph2	Trident-II		
Model	3290	3295	3920	3922	3930	as5600_52x	3780	as4600_54t	3297	5101	5401	as6701_32x

Chip	Firebolt3								Triumph2	Trident-II		
output<PORT_ID>	√	√	√	√	√	√	√	√	√	√	√	√
mod_dl_src	√	√	√	√	√	√	√	√	√	√	√	√
mod_dl_dst	√	√	√	√	√	√	√	√	√	√	√	√
mod_vlan_vid	√	√	√	√	√	√	√	√	√	√	√	√
mod_vlan_pcp	√	√	√	√	√	√	√	√	√	√	√	√
mod_nw_tos	√	√	√	√	√	√	√	√	√	√	√	√
push_vlan	√	√	√	√	√	√	√	√	√	√	√	√
pop_vlan	√	√	√	√	√	√	√	√	√	√	√	√
strip_vlan	√	√	√	√	√	√	√	√	√	√	√	√
push_pbb	X	X	√	√	√	√	√	X	√	√	√	√
pop_pbb	X	X	√	√	√	√	√	X	√	√	√	√
set_queue	√	√	√	√	√	√	√	√	√	√	√	√
push_mpls	X	X	√	√	√	√	√	X	√	√	√	√
pop_mpls	X	X	√	√	√	√	√	X	√	√	√	√
mod_nw_src	X	X	X	X	X	X	X	X	X	√	√	√
mod_nw_dst	X	X	X	X	X	X	X	X	X	√	√	√
mod_tp_src	X	X	X	X	X	X	X	X	X	√	√	√
mod_tp_dst	X	X	X	X	X	X	X	X	X	√	√	√

The following actions are not supported.

Different modification for a different bucket

eg.

bucket=mod_dl_src:22:11:11:11:11:11,output:2,bucket=mod_dl_src:22:22:22:22:22:22,output:3

ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>

> In PicOS OVS, each meter only support configure one meter band.
>
> The counters of one meter are the same as the flow entry counters which the meter applied.

PicOS OVS supports meters from Openflow 1.3. In different Hardware Models, the maximum count of meters that PicOS OVS supports is different. User can use the command to check the maximum count.

```
admin@PicOS-OVS$ovs-ofctl meter-features br0
OFPST_METER_FEATURES reply (OF1.4) (xid=0x2):
max_meter:2048 max_bands:1 max_color:3
band_types: drop dscp_remark
capabilities: kbps burst stats
```

ovs-ofctl add-meter <*bridge*> meter=<*id*>,kbps*[,burst,stats]*,band=type=drop,rate=<*rate*>*[,burst_size=<size>][,prec_level=<level>]*

Add a meter, the type=drop.

Example:

Without burst size. Limit the rate as 30000kbps.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=30000
```

With burst size. Limit the rate as 30000kbps.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=drop,rate=30000,burst_size=30000
```

ovs-ofctl add-meter <*bridge*> meter=<*id*>,kbps*[,burst,stats]*,band=type= dscp_remark,rate=<*rate*>,prec_level=<*level*>*[,burst_size=<size>]*

Add a meter, the type=dscp_remark.

Example:

Without burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,band=type=dscp_remark,rate=30000,prec_level=14
```

With burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=dscp_remark,rate=30000,prec_level=14,burst_size
```

If one meter applies to multiple flow entries, all the flow entries will share the meter rate.

Example:

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=30000
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:11,dl_type=0x0800,a
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=12,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:22,dl_type=0x0800,a
```

The result: the total rate in port te-1/1/13 is limit to 30000 kbps.

ovs-ofctl bundle <bridge> <bundle>

PicOS OVS supports bundles from version 2.3.

User can add a bundle with the format as follows:

ovs-ofctl bundle <bridge> "[open:bundle_id=<id>,]add:bundle_id=<id>,message=<message>[,add:bundle_id=<id>,message=<message>...][,close:bundle_id=<id>],commit:bundle_id=<id>"

Using bundles is to group related state changes on a switch so that all changes are applied together, or that none of them is applied. The second goal is to better synchronize changes across a set of OpenFlow switches. Bundles can be prepared and pre-validated on each switch and applied at the same time.

PicOS OVS supports applying 10 bundles maximum at the same time. And the maximum messages is 100 of each bundle.
Also supports port/flow/group/meter-mods at present.

Flow-mod

message=add-flow <match><,actions>

User can add a flow by bundle.
Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=add-flow in_port=1,dl_src=22:11:11:1
```

messag=mod-flows <match><,actions>

Modify flows by bundle.

message=del-flows <match>

Delete flows by bundle.
Example:

Delete the flows that match the field.

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-flows in_port=1,commit:bundle_id
```

Delete all flows in br0.

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-flows,commit:bundle_id=1"
```

Group-mod

message=add-group group_id=<id>,type=<type>,bucket=<actions>[,bucket=<actions>]

Add groups by bundle.

Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=add-group group_id=1,type=all,bucket
```

message=mod-group group_id=<id>,type=<type>,bucket=<actions>[,bucket=<actions>]

Modify a group by bundle.

message=del-groups group_id=<id>

Delete groups by bundle.
Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-groups ,commit:bundle_id=1"
```

Meter-mod

message=add-meter meter=<id> kbps[,burst,stats],band=type=<type>,rate=<rate>[,burst_size=<size>,prec_level=<level>]

Add meter by bundle.

message=mod-meter meter=<id> kbps[,burst,stats],band=type=<type>,rate=<rate>[,burst_size=<size>,prec_level=<level>]

Modify meter by bundle.

message=del-meter meter=<id>

Delete meter that meter=<id>.

Port-mod

message=mod-port <port> <down/up/no-receive/receive/no-forward/forward/no-packet-in/packet-in>

Modify port state, the configure must be one of 'down/up/no-receive/receive/no-forward/forward/no-packet-in/packet-in'.

Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 'open:bundle_id=1,add:bundle_id=1,message=mod-port te-1/1/1 no-packet-in,comm
```

Multiple bundles

User can apply multiple bundles at the same time. Each bundle has its own open/add/close/commit/discard.
Example:

```
root@PicOS-OVS$ovs-ofctl bundle br-iris "open:bundle_id=1,open:bundle_id=2,add:bundle_id=1,message=add-flow dl_src=
```

ovs-ofctl del-flows <bridge> <flow>

Delete the flow entries from the flow table of <*bridge*>. If the *[flow]* is omitted, delete all flows in <*bridge*>, otherwise, will delete the matched flows.

ovs-ofctl del-group <bridge> [group_id=<id>]

Delete group in <bridge>. If the group_id is specified, the group that <group_id> in <bridge> will delete, otherwise, all groups in <bridge> will be cleared.
Example:

```
admin@PicOS-OVS$ovs-ofctl del-groups br0 group_id=2
admin@PicOS-OVS$ovs-ofctl del-groups br0
```

ovs-ofctl del-meter <bridge> meter=<id>

Delete the meter that meter=<id> in <bridge>.

ovs-ofctl del-meters <bridge>

Delete all the meters in <bridge>.

ovs-ofctl dump-desc <bridge>

Prints <*bridge*> description, including manufacturer, hardware, software, serial number and dp description.

ovs-ofctl dump-flows <bridge> <flow>

Prints flow.entries of <bridge>. With the *[flow]* specified will only print the matching flow. If the *[flow]* is omitted, all flow entries of the bridge will be printed.

ovs-ofctl dump-ports <bridge> <port>

Prints the port statistics of <*bridge*>. If the port is specified, only the port statistics of the bridge will be printed, otherwise, will print all the ports statistics.

ovs-ofctl dump-ports-desc <bridge>

Prints port statistics. Will show detail information about the interfaces in this bridge, including the state, peer and speed information,etc. The information printed by this command is a subset of command 'ovs-ofctl show ***<bridge>'.***

ovs-ofctl dump-tables <bridge>

Prints <*bridge*> all table stats. Including all 254 tables.

ovs-ofctl dump-tables-desc <bridge>

Prints the descriptions of tables of <bridge>.

ovs-ofctl mod-flows <bridge> <flow>

Modify the actions of matching flows in the *<bridge>*.

ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>

Modify a group if the group entry with the specified group identifier already resides in the group table. If the group identifier does not exist, the group will add in group table successfully.
Example:

```
admin@PicOS-OVS$ovs-ofctl mod-group br0 group id=100,type=indirect,bucket=mod dl src=00:00:00:99:11:11,mod dl dst=00:00:00:99:22:22
```

ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>

Modify a meter if the meter entry with the specified meter identifier already exists.

The format is shown as follows:

ovs-ofctl mod-meter <bridge> meter=<id>,kbps[,burst,stats],band=type=<type>,rate=<rate>,burst_size=<size>,prec_level=<level>

ovs-ofctl mod−port <bridge> <iface> <action>

Modify behaviors of port *<iface>* in *switch*. *<iface>* can be an OpenFlow port number or name, or the **LOCAL** port name. The *<action>* can be as follows:

ovs-ofctl mod-port <bridge> <iface> up

ovs-ofctl mod-port <bridge> <iface> down

Enable or disable the port link status.

ovs-ofctl mod-port <bridge> <iface> receive

ovs-ofctl mod-port <bridge> <iface> no−receive

Allow or disallow this interface to receive traffic. By default, receiving is allowed.

ovs-ofctl mod-port <bridge> <iface> forward

ovs-ofctl mod-port <bridge> <iface> no−forward

Allow or disallow traffic forwarding on this interface. By default, forwarding is allowed.

ovs-ofctl mod-port <bridge> <iface> flood

ovs-ofctl mod-port <bridge> <iface> no−flood

Controls whether the interface is to flood the received traffic or not. By default, flooding is enabled. Disabling flooding is primarily useful to prevent loops when a spanning tree protocol is not in use.

ovs-ofctl mod-table <bridge> <table> <mod>

ovs-ofctl mod-table <bridge> <table> evict

Enable eviction on <table> of <bridge>. Eviction adds a mechanism enabling the switch to automatically eliminate entries of lower importance to make space for newer entries. This enables smoother degradation of behavior when the table is full.
To enable eviction on all tables, user can set the <table> as 'all'.

ovs-ofctl mod-table <bridge> <table> vacancy:<range>

Configure the vacancy <range> on <table> of <bridge>. The vacancy event adds a mechanism enabling the controller to get an early warning based on a capacity threshold chosen by the controller. This allows the controller to react in advance and avoid getting the table full. If user wants to configure vacancy range on all tables, set the <table> as 'all'.
The syntax of <range> as <low..high>.

ovs-ofctl mod-table <bridge> <table> clear

Clear the eviction or vacancy on <table> of <bridge>. If user wants to clear eviction on all tables, set the <table> as 'all'.

ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]

Print packets received from <bridge>.

ovs-ofctl show <bridge>

Show OpenFlow information on <*bridge*>, including OpenFlow features and port descriptions.

ovs-ofctl snoop <bridge>

ovs-ofctl snoop br0

This command snoops the bridge for open flow messages exchanged with the controller. It can be used to debug flow installations, modifications and packet_in and packet_out messages on the bridge. This command executes in a continuous loop. ^C should be used to break the display output.

```
admin@SpineA-OVS$ovs-ofctl snoop br0
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_PACKET_IN (OF1.3) (xid=0x0): cookie=0x0 total_len=1516 in_port=1 (via action) data_len=1516 (unbuffered)
udp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29:70:2e:b8,nw_src=100.0.(
OFPT_PACKET_OUT (OF1.3) (xid=0x4c): in_port=CONTROLLER actions=output:2 data_len=1516
udp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29:70:2e:b8,nw_src=100.0.(
OFPT_FLOW_MOD (OF1.3) (xid=0x4d): ADD priority=25000,in_port=1,dl_vlan=100,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29
OFPT_BARRIER_REQUEST (OF1.3) (xid=0x4e):
OFPT_BARRIER_REPLY (OF1.3) (xid=0x4e):
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_PACKET_IN (OF1.3) (xid=0x0): cookie=0x0 total_len=64 in_port=2 (via action) data_len=64 (unbuffered)
arp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29:fd:75:ae,arp_spa=100.0
OFPT_PACKET_OUT (OF1.3) (xid=0x4f): in_port=CONTROLLER actions=output:1 data_len=64
arp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29:fd:75:ae,arp_spa=100.0
OFPT_FLOW_MOD (OF1.3) (xid=0x50): ADD priority=25000,in_port=2,dl_vlan=100,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29
OFPT_BARRIER_REQUEST (OF1.3) (xid=0x51):
OFPT_BARRIER_REPLY (OF1.3) (xid=0x51):
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
```

In case of error conditions, a hex dump of the erroneous packet is displayed.

```
admin@XorPlus$ovs-ofctl snoop br0



OFPT_PACKET_OUT (OF1.3) (xid=0x375f4): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f5): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375f6): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f7): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375f8): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f9): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375fa): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375fb): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375fc): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375fd): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375fe): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375ff): in_port=CONTROLLER actions=output:3 data_len=81
```

```
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPST_PORT request (OF1.3) (xid=0x26): port_no=ANY
OFPST_PORT reply (OF1.3) (xid=0x26): 4 ports
  port  1: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604176.668s
  port  2: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604121.342s
  port  3: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604091.091s
  port LOCAL: rx pkts=8, bytes=816, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=934668.169s
OFPST_FLOW request (OF1.3) (xid=0x37601):
OFPST_FLOW reply (OF1.3) (xid=0x37601):
 cookie=0x1f00007eaab36a, duration=836.005s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,arp a
 cookie=0x1f00007eaab36a, duration=836.005s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=5,arp actio
 cookie=0x1f00007eaa9ce4, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=5,ip actions
 cookie=0x1f00007ccd1ab0, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,dl_ty
 cookie=0x1f00007cced5a6, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,dl_ty
OFPT_FLOW_MOD (OF1.3) (xid=0x0): ***decode error: OFPBMC_BAD_PREREQ***
OFPT_ERROR (OF1.3) (xid=0x0): OFPBMC_BAD_PREREQ
OFPT_FLOW_MOD (OF1.3) (xid=0x0):
(***truncated to 64 bytes from 88***)
00000000  04 0e 00 58 00 00 00 00-00 1f 00 00 a5 d7 3f 26 |...X.........?&|
00000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 05 |................|
00000020  ff ff ff ff ff ff ff ff-ff ff ff ff 00 01 00 00 |................|
00000030  00 01 00 10 80 00 19 08-e0 00 00 00 f0 00 00 00 |................|
OFPT_PACKET_OUT (OF1.3) (xid=0x37604): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37605): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x37606): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37607): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x37608): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37609): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPST_GROUP request (OF1.3) (xid=0x3e6b): group_id=ALL
OFPST_GROUP reply (OF1.3) (xid=0x3e6b):
OFPST_GROUP_DESC request (OF1.3) (xid=0x3e6c): group_id=ALL
OFPST_GROUP_DESC reply (OF1.3) (xid=0x3e6c):
^C2015-09-15T17:36:40Z|00001|fatal_signal|WARN|terminating with signal 2 (Interrupt)
```

ovs-ofctl replace-flows <bridge> <file>

ovs-ofctl replace-flows <bridge> <file>

Using this command, you can replace existing flows in the bridge.

Example:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#13 normal permanent recirc_id=0,in_port=10, actions:8,9
#12 normal_d permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl replace-flows br0 file2.txt
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#14 normal permanent recirc_id=0,in_port=8,dl_dst=22:22:22:22:22:33, actions:10
#15 normal permanent recirc_id=0,in_port=8,dl_dst=22:22:22:22:22:22, actions:9
```

ovs-ofctl diff-flows <source1> <source2>

ovs-ofctl diff-flows <source1> <source2>

Compare flows from two sources, you can also compare flows from a bridge and a source.

Example:

```
admin@PicOS-OVS$ls
file1.txt file2.txt
admin@PicOS-OVS$cat file1.txt
in_port=9,dl_vlan=10,actions=output:8
admin@PicOS-OVS$
admin@PicOS-OVS$cat file2.txt
in_port=8,dl_dst=22:22:22:22:22:22,actions=output:9
in_port=8,dl_dst=22:22:22:22:22:33,actions=output:10
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl diff-flows file2.txt file1.txt
-in_port=8,dl_dst=22:22:22:22:22:22 actions=output:9
-in_port=8,dl_dst=22:22:22:22:22:33 actions=output:10
+in_port=9,dl_vlan=10 actions=output:8
```

ovs-ofctl add-groups <bridge> <file>

ovs-ofctl add-groups <bridge> <file>

Add groups to the switch from a file.

Example:

```
admin@PicOS-OVS$cat group.txt
group_id=1,type=all,bucket=output:8
group_id=2,type=select,bucket=output:9,bucket=output:10
admin@PicOS-OVS$ovs-ofctl add-groups br0 group.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-groups br0
OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
group_id=1,type=all,bucket=actions=output:8
group_id=2,type=select,bucket=actions=output:9,bucket=actions=output:10
admin@PicOS-OVS$
admin@PicOS-OVS$
```

ovs-ofctl queue-get-config <bridge> <port>

ovs-ofctl queue-get-config <bridge> <port>

Print queue information for specified port.

Example:

```
admin@PicOS-OVS$ovs-ofctl queue-get-config br0 ge-1/1/8
OFPT_QUEUE_GET_CONFIG_REPLY (OF1.4) (xid=0x4): port=8
queue 0: port=8 min_rate:1.2% max_rate:1.2%
queue 7: port=8 min_rate:1.2% max_rate:1.2%
```

ovs-ofctl meter-stats <bridge> [meter]

ovs-ofctl meter-stats <bridge> [meter]

Print meter statistics.

Example:

```
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:100 flow_count:0 packet_in_count:0 byte_in_count:0 duration:346.419s bands:
0: packet_count:0 byte_count:0
```

ovs-ofctl meter-features <bridge>

ovs-ofctl meter-features <bridge>

Print meter features.

Example:

```
admin@PicOS-OVS$ovs-ofctl meter-features br0
OFPST_METER_FEATURES reply (OF1.4) (xid=0x2):
max_meter:100 max_bands:1 max_color:3
band_types: drop dscp_remark
capabilities: kbps burst stats
```

ovs-ofctl dump-meters <bridge>

ovs-ofctl dump-meters <bridge>

Print all meter configurations.

ovs-ofctl dump-meter <bridge> [meter_id]

Print METER configuration of this meter_id.

ovs−vsctl Commands

The command **ovs-vsctl** is a utility for querying and configuring the Open vSwitch. The Open vSwitch configuration is kept in a database managed by the **ovsdb-server** process.The **ovs-vsctl** command connects to **ovsdb-server**, which maintains the Open vSwitch configuration database. Using this connection, **ovs-vsctl** queries and applies changes to the database, based on the supplied commands.

See **ovs-vsctl** help for more information about the utility.

```
admin@PICOS-OVS:~$ ovs-vsctl --help
ovs-vsctl: ovs-vswitchd management utility
usage: ovs-vsctl [OPTIONS] COMMAND [ARG...]

Open vSwitch commands:
  init                        initialize database, if not yet initialized
  show                        print overview of database contents
  emer-reset                  reset configuration to clean state

Bridge commands:
  add-br BRIDGE               create a new bridge named BRIDGE
  add-br BRIDGE PARENT VLAN   create new fake BRIDGE in PARENT on VLAN
  del-br BRIDGE               delete BRIDGE and all of its ports
  list-br                     print the names of all the bridges
  br-exists BRIDGE            exit 2 if BRIDGE does not exist
  br-to-vlan BRIDGE           print the VLAN which BRIDGE is on
  br-to-parent BRIDGE         print the parent of BRIDGE
  br-set-external-id BRIDGE KEY VALUE  set KEY on BRIDGE to VALUE
  br-set-external-id BRIDGE KEY  unset KEY on BRIDGE
  br-get-external-id BRIDGE KEY  print value of KEY on BRIDGE
  br-get-external-id BRIDGE  list key-value pairs on BRIDGE

Port commands (a bond is considered to be a single port):
  list-ports BRIDGE           print the names of all the ports on BRIDGE
  add-port BRIDGE PORT        add network device PORT to BRIDGE
  add-bond BRIDGE PORT IFACE...  add bonded port PORT in BRIDGE from IFACES
  del-port [BRIDGE] PORT      delete PORT (which may be bonded) from BRIDGE
  port-to-br PORT             print name of bridge that contains PORT

Interface commands (a bond consists of multiple interfaces):
  list-ifaces BRIDGE          print the names of all interfaces on BRIDGE
  iface-to-br IFACE           print name of bridge that contains IFACE

Controller commands:
  get-controller BRIDGE      print the controllers for BRIDGE
  del-controller BRIDGE      delete the controllers for BRIDGE
  set-controller BRIDGE TARGET...  set the controllers for BRIDGE
  get-fail-mode BRIDGE       print the fail-mode for BRIDGE
  del-fail-mode BRIDGE       delete the fail-mode for BRIDGE
  set-fail-mode BRIDGE MODE  set the fail-mode for BRIDGE to MODE

Manager commands:
  get-manager                print the managers
  del-manager                delete the managers
  set-manager TARGET...      set the list of managers to TARGET...

SSL commands:
  get-ssl                     print the SSL configuration
  del-ssl                     delete the SSL configuration
  set-ssl PRIV-KEY CERT CA-CERT  set the SSL configuration

Switch commands:
  emer-reset                  reset switch to known good state

Database commands:
  list TBL [REC]              list RECord (or all records) in TBL
  find TBL CONDITION...       list records satisfying CONDITION in TBL
  get TBL REC COL[:KEY]       print values of COLumns in RECord in TBL
  set TBL REC COL[:KEY]=VALUE set COLumn values in RECord in TBL
```

```
  add TBL REC COL [KEY=]VALUE add (KEY=)VALUE to COLumn in RECord in TBL
  remove TBL REC COL [KEY=]VALUE  remove (KEY=)VALUE from COLumn
  clear TBL REC COL           clear values from COLumn in RECord in TBL
  create TBL COL[:KEY]=VALUE  create and initialize new record
  destroy TBL REC             delete RECord from TBL
  wait-until TBL REC [COL[:KEY]=VALUE]  wait until condition is true
Potentially unsafe database commands require --force option.

Options:
  --db=DATABASE               connect to DATABASE
                              (default: unix:/ovs/var/run/openvswitch/db.sock)
  --no-wait                   do not wait for ovs-vswitchd to reconfigure
  --retry                     keep trying to connect to server forever
  -t, --timeout=SECS          wait at most SECS seconds for ovs-vswitchd
  --dry-run                   do not commit changes to database
  --oneline                   print exactly one line of output per command

Pica commands:
  show-running-config                           print current ovsdb config
  show-valid-port [FRONT]                       print all valid ports or one
  set-port-breakout ALL|FRONT TRUE|FALSE        use breakout cable or not
  set-port-name FRONT [1,4]=default|XXX         modify name of sub-port on FRONT
  set-match-mode MODE:OPTIONS=PRIORITY          set match-modes
  show-match-mode                               print current match-modes
  set-gtp-udp-dst-ports PORT...                 set gtp udp ports, PORT is up to 4
  show-gtp-udp-dst-ports                        show gtp udp ports
  set-match-vxlan-vni-enable TRUE|FALSE         enable or disable vxlan vni matching
  show-match-vxlan-vni                          show vxlan vni matching
  set-vxlan-udp-dst-port [1, 65535]             set vxlan udp destination port
  show-vxlan-udp-dst-port                       show vxlan udp destination port
  set-vntag-ethertype [0x6000, 0xffff]          set VN tag ethertype
  show-vntag-ethertype                          show VN tag ethertype
  set-snmp-enable TRUE|FALSE                    enable or disable snmp
  show-snmp                                     show snmp
  set-snmp-trap-targets    IPv4(s)              set snmp trap targets
  show-snmp-trap-targets                        show snmp trap targets
  set-snmp-community-name                       set snmp agent community name
  show-snmp-community-name                      show snmp agent community name
  set-cos-map TRUE|FALSE                        enable or disable cos-mapping
  show-cos-map [IFACE]                          show cos-mapping
  set-vlan-priority-cos-map TRUE|FALSE          enable or disable vlan-priority-cos-mapping
  show-vlan-priority-cos-map                    show vlan-priority-cos-mapping
  set-egress-mode TRUE|FALSE [TABLE]            set egress mode
  show-egress-mode                              show egress-mode
  set-combinated-mode TRUE|FALSE                enable or disable combinated-mode
  show-combinated-mode                          show combinated-mode
  set-l2gre-key-length                          set l2gre key length
  show-l2gre-key-length                         show l2gre key length
  set-proxy-arp TRUE|FALSE SUBNETS              set proxy arp
  show-proxy-arp                                show proxy arp
  set-proxy-icmpv6 TRUE|FALSE SUBNETS           set proxy icmpv6 for NS/NA
  show-proxy-icmpv6                             show proxy icmpv6
  set-l2-mode TRUE|FALSE [TABLE]                set l2 mode
  show-l2-mode                                  show l2 mode
  set-l3-mode TRUE|FALSE [TABLE]                set l3 mode
  show-l3-mode                                  show l3 mode
  set-l2-l3-buffer-mode [0, 5]                  set l2/l3 buffer mode(0-5)
  show-l2-l3-buffer-mode                        show l2/l3 buffer mode
  set-l2-l3-preference TRUE|FALSE               set l2/l3 flow preference
  show-l2-l3-preference                         show l2/l3 flow preference
  set-max-ecmp-ports NUM                        set l3 max ecmp ports to NUM(2~32 and a power of 2)
  show-max-ecmp-ports                           show l3 max ecmp ports
  set-lag-advance-hash-mapping-fields FIELDS    set hash fields of advance hash-mapping
  show-lag-advance-hash-mapping-fields          show hash fields of advance hash-mapping
  set-udf-mode MODE                             set udf mode, MODE's format is udfN(l2|l3,offset=OFS,length=LEN),.
                                                only up to 4 udfs(udf0,udf1,udf2,udf3) are supported
  show-udf-mode                                 show udf mode
  set-max-resilient-hash-lag-count COUNT        set lag-max-resilient-hash-lag-count.
                                                COUNT is max count of lags which,
                                                can be set to resilient hash,
```

```
                                                the valid value of COUNT is
                                                1, 2, 4, 8, 16, 32, 64.
                                                The default value is 1.
  show-max-resilient-hash-lag-count             show lag-max-resilient-hash-lag-count.
  set-macro-udf MODE                            set macro udf mode instead of offset and length, look up show udf t
  show-macro-udf                                show macro udf mode
  show-udf-field                                options for macro udf
  set-egress-mc-queue-dynamic [0,7] TRUE|FALSE  set certain queue id multicast dynamic buffer enable
  set-egress-shared-queue-ratio [0,7] [0,100]   set certain queue id shared buffer ratio
  show-egress-shared-queue-ratio                show added queue id shared buffer ratio
  set-loopback-enable TRUE|FALSE                set loopback enable or disable
  set-option-match-vlan-type TRUE|FALSE         enable or disable matching untagged pakcets
  show-option-match-vlan-type                   show vlan format enable or disable
  set-select-group-hash-fields [FIELDS]         set select-group-hash-fields
  show-select-group-hash-fields                 show current select-group-hash-fields
  set-flow-handling-mode [MODE]                 set flow-handling-mode
  show-flow-handling-mode                       show current flow-handling-mode
  set-rdbgc4 [TYPE]                             set rdbgc4
  show-rdbgc4                                   show current rdbgc4
  set-lag-members-sorted                        set lag members sorted
  show-lag-members-sorted                       show lag members sorted
  set-group-ranges [GROUPS]                     set special groups(lag-select-groups, ecmp-select-groups,
                                                ingress-mirror-groups, egress-mirror-groups) ranges
  show-group-ranges                             show current group ranges
  set-meter-ranges [METERS]                     set special meters(egress-meter) ranges
  show-meter-ranges                             show current meter ranges
  set-l3-ecmp-hash-fields FIELDS                set l3 ecmp hash fields
  show-l3-ecmp-hash-fields                      show l3 ecmp hash fields
  set-l3-egress-keep-fields [FIELDS]            set default keep fields in l3 egress interface
  show-l3-egress-keep-fields                    show default keep fields in l3 egress interface
  disable-extend-group TRUE|FALSE               disable or enable extend group for arp/mpls flows
  show-extend-group                             show extend group config
  set-symmetric-hash [LAG|ECMP] TRUE|FALSE      disable or enable symmetric hash
  show-symmetric-hash                           show symmetric hash config
  set-flow-counter-mode both|bytes|packets      set flow counter mode
  show-flow-counter-mode                        show flow counter mode
  set-ttp-enable TRUE|FALSE                     set ttp module enable or disable
  set-ttp-file FILE                             set ttp file name
  show-ttp                                      show ttp status and file name
  set-counter-interval [10,1000]                set counter interval
  show-counter-interval                         show counter interval
  display-settings                              show the configurations in OVSDB through ovs-vsctl comands

Logging options:
  -vSPEC, --verbose=SPEC   set logging levels
  -v, --verbose            set maximum verbosity level
  --log-file[=FILE]        enable logging to specified FILE
                           (default: /ovs/var/log/openvswitch/ovs-vsctl.log)
  --syslog-target=HOST:PORT  also send syslog msgs to HOST:PORT via UDP
  --no-syslog              equivalent to --verbose=vsctl:syslog:warn

Active database connection methods:
  tcp:IP:PORT              PORT at remote IP
  ssl:IP:PORT              SSL PORT at remote IP
  unix:FILE                Unix domain socket named FILE
Passive database connection methods:
  ptcp:PORT[:IP]           listen to TCP PORT on IP
  pssl:PORT[:IP]           listen for SSL on PORT on IP
  punix:FILE               listen on Unix domain socket FILE
PKI configuration (required to use SSL):
  -p, --private-key=FILE   file with private key
  -c, --certificate=FILE   file with certificate for private key
  -C, --ca-cert=FILE       file with peer CA certificate

Other options:
  -h, --help                  display this help message
  -V, --version               display version information
admin@PICOS-OVS:~$
```

See ovs-vsctl main page for detailed syntax and additional information.

```
admin@Switch$man ovs-vsctl
ovs-vsctl(8)                                  Open vSwitch Manual                                  ovs-vs
NAME
       ovs-vsctl - utility for querying and configuring ovs-vswitchd
SYNOPSIS
       ovs-vsctl [options] -- [options] command [args] [-- [options] command [args]]...
DESCRIPTION
       The  ovs-vsctl  program  configures ovs-vswitchd(8) by providing a high-level interface to its configuratio
       base.  See ovs-vswitchd.conf.db(5) for comprehensive documentation of the database schema.
       ovs-vsctl connects to an ovsdb-server process that maintains an Open vSwitch configuration database.   Usin
       connection, it queries and possibly applies changes to the database, depending on the supplied commands.  Th
       it applied any changes, by default it waits until ovs-vswitchd has finished reconfiguring itself before it
       (If you use ovs-vsctl when ovs-vswitchd is not running, use --no-wait.)
       ovs-vsctl  can  perform any number of commands in a single run, implemented as a single atomic transaction a
       the database.
       The ovs-vsctl command line begins with global options (see OPTIONS below for details).   The  global  optio
       followed by one or more commands.  Each command should begin with -- by itself as a command-line argument, t
       arate it from the following commands.  (The -- before the first command is optional.)  The command  itself
       with  command-specific  options,  if  any, followed by the command name and any arguments.  See EXAMPLES bel
       syntax examples.
   Linux VLAN Bridging Compatibility
       The ovs-vsctl program supports the model of a bridge implemented by Open vSwitch, in which a  single  bridge
       ports  ports  on  multiple  VLANs.   In  this model, each port on a bridge is either a trunk port that poter
       passes packets tagged with 802.1Q headers that designate VLANs or it is assigned a single implicit  VLAN  th
       never tagged with an 802.1Q header.
       For  compatibility  with  software designed for the Linux bridge, ovs-vsctl also supports a model in which t
       associated with a given 802.1Q VLAN is segregated into a separate bridge.  A special form of  the  add-br  c
       (see below) creates a ``fake bridge'' within an Open vSwitch bridge to simulate this behavior.  When such a
       bridge'' is active, ovs-vsctl will treat it much like a bridge separate from its ``parent bridge,'' but the
       implementation in Open vSwitch uses only a single bridge, with ports on the fake bridge assigned the implici
       of the fake bridge of which they are members.  (A fake bridge for VLAN 0 receives packets that have no 802.1
       or a tag with VLAN 0.)
<Some output omitted>
```


- Bridge Commands
  - ovs-vsctl add-br
  - ovs-vsctl del-br
  - ovs-vsctl list-br
  - ovs-vsctl set bridge
- Port Commands
  - ovs-vsctl add-port
  - ovs-vsctl list-ports
  - ovs-vsctl del-port
- Controller commands
- Database commands
- Interface commands
- Mirror Commands
- NetFlow Commands
- Open vSwitch commands
- Match-mode Command
- QoS_queue Commands
- sFlow commands
- Cos-map Command
- Egress-mode Command
- Set-flow-counter-mode Command
- Combinated-mode Command
- DSCP Commands

Bridge Commands

These commands are used to create and configure Open vSwitch bridges. Commands for displaying the status of OpenvSwitch bridges are also provided.

- ovs-vsctl add-br
- ovs-vsctl del-br
- ovs-vsctl list-br
- ovs-vsctl set bridge

ovs-vsctl add-br

To create a new bridge, use the **ovs-vsctl add-br** command. The new bridge initially has no ports, other than the bridge itself.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **add-br** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--may-exist	Without the **--may-exist** option, attempting to create bridge that already exists creates an error. With the **--may-exist** option, the command does nothing if the bridge already exists as a real bridge.
bridge	Arbitrary bridge name.

Examples

The following example creates a new bridge named **br0**:

```
admin@Switch$ovs-vsctl --may-exist add-br br0
```

ovs-vsctl del-br

To delete a bridge and all of its ports, use the **ovs-vsctl del-br** command. If the bridge is real, this command also deletes any fake bridges that were created with the bridge as parent, and all of their ports.

Syntax

ovs-vsctl [*options*] [**--if-exists**] **del-br** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--if-exist	Without the **--if-exists** option, attempting to delete a bridge that does not exist creates an error. With the **--if-exists** option, attempting to delete a bridge that does not exist has no effect.
bridge	Name of the bridge to be deleted.

Examples

The following example deletes the bridge named **br0**:

```
admin@Switch$ovs-vsctl --if-exists del-br br0
```

ovs-vsctl list-br

To list all existing real and fake bridges, use the **ovs-vsctl list-br** command.

Syntax

ovs-vsctl [*options*] [**--real** | **--fake**] **list-br**

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--real	List only real bridges.
--fake	List only fake bridges.

Examples

The following example lists bridges, where only a single real bridge **br0** exists:

```
admin@Switch$ovs-vsctl list-br
br0
admin@Switch$ovs-vsctl --fake list-br
admin@Switch$ovs-vsctl --real list-br
br0
```

ovs-vsctl set bridge

Examples

The following examples provide typical usage of the **ovs-vsctl set bridge** command.

Disabling In-Band Management

By default, remote in-band management is enabled on Open vSwitch. You can disable in-band management by setting the **other-config** parameter **disable-in-band** to **true**. And the configurations will apply in all the controllers in the bridge.

The following example disables in-band management of bridge *br0*:

```
admin@Switch$ovs-vsctl set bridge br0 other-config:disable-in-band=true
```

The following example enables in-band management of bridge *br0*:

```
admin@Switch$ovs-vsctl set bridge br0 other-config:disable-in-band=false
```

Port Commands

ovs-vsctl *[--OPTION]* add-port *<bridge> <port> [ARG...] [--[OPTION] <COMMAND> [ARGs]]*

Add a new port named *<port>* to *<bridge>*. Including physic port, LAG port and GRE tunnel.

Physical Port

Example:

Add a physical port.

```
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set interface ge-1/1/1 type=pica8
```

Add a physical port and configure special link_speed.

```
ovs-vsctl add-port br0 te-1/1/49 vlan_mode=trunk tag=1 trunks=2000,4094 -- set interface te-1/1/49  type=pica8 opt
```

Crossflow Port

Example:

When adding a crossflow port the vlan_mode and the trunks should be set via CLI.

```
ovs-vsctl add-port br0 te-1/1/1 -- set interface te-1/1/1 type=crossflow
```

LAG Port

Example:

Add a lag interface:

```
root@PicOS-OVS#ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set Interface ae1 type=pica8_la
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lag_type=static
```

Modify the numbers of the lag

```
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:members=ge-1/1/2,ge-1/1/3
```

LACP Port

Example:

Add a lacp port and configure the parameter.

```
root@PicOS-OVS#ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set Interface ae1 type=pica8_la
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lag_type=lacp
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:members=ge-1/1/2,ge-1/1/3
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-system-id=00:11:11:11:11:11
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-system-priority=32768
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-time=fast
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-time=slow
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-mode=active
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-mode=passive
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-port-id=2
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-port-priority=32768
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-aggregation-key=0
```

GRE Port

Example:

Add a GRE port.

```
ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.61.10 options:local_ip=10
```

ovs-vsctl *[--OPTION]* list-ports *<bridge>*

Print the names of all the ports on *<bridge>*.

Example:

```
ovs-vsctl list-ports br0
```

ovs-vsctl *[--OPTION]* del-port *<bridge>* *<port>*

Delete the port named *<port>* from *<bridge>*.

Example:

```
ovs-vsctl del-port br1 ge-1/1/1
```

ovs-vsctl *[--OPTION]* port-to-br *<port>*

Print name of the bridge which contrains the special *<port>*.

Example:

```
ovs-vsctl port-to-br ge-1/1/1
```

VXLAN Port

Example:

Add a VXLAN port.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.
```

L2GRE Port

Example:

Add a L2GRE port.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.
```

- ovs-vsctl add-port
- ovs-vsctl list-ports
- ovs-vsctl del-port

ovs-vsctl add-port

To create a new port on the bridge from the network device of the same name, use the **ovs-vsctl add-port** command.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **add-port** *bridge port* [*args*]

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced here.
--may-exist	Without the **--may-exist** option, attempting to create a port that exists is an error. With the **--may-exist** option, this command does nothing if the port already exists in the bridge and is not a bonded port.
bridge	Bridge name.
port	Port name.
args	Optional arguments configure additional parameters for the port. For example, tag=9 would make the port an access port for VLAN 9. The syntax is the same as that for the **ovs-vsctl set port** command.

Examples

The following example adds the ge-1/1/1 port to bridge br0:

```
admin@Switch$ovs-vsctl add-port br0 ge-1/1/1
```

Add Bond Ports

PicOS support bond multiple ports as in_port or output, and this virtual port will not influnce each physical port forwarding packets.

Examples

Bonding port ge-1/1/1 ~ ge-1/1/4 as one port.

```
// add ports
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set Interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set Interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set Interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 -- set Interface ge-1/1/4 type=pica8

// add bond ports
ovs-vsctl add-port br0 bond1 -- set Interface bond1 type=pica8_bond
ovs-vsctl set Interface bond1 options:members=ge-1/1/2,ge-1/1/3,ge-1/1/4

// add flows
ovs-ofctl add-flow br0 in_port=2049,actions=1
ovs-ofctl add-flow br0 in_port=1,actions=2049
```

ovs-vsctl list-ports

To list all of the ports within a bridge, use the **ovs-vsctl list-ports** command. The local bridge port is not included in the list.

Syntax

ovs-vsctl [*options*] **list-ports** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced here.
bridge	Bridge name.

Examples

The following example lists ports within the bridge **br0**:

```
admin@Switch$ovs-vsctl list-ports br0
```

ovs-vsctl del-port

To create a new port on the bridge from the network device of the same name, use the **ovs-vsctl add-port** command.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **del-port** *bridge port*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--may-exist	Without the **--may-exist** option, attempting to create a port that exists is an error. With the **--may-exist** option, this command does nothing if the port already exists in the bridge and is not a bonded port.
bridge	Bridge name.
port	Port name.

Examples

The following example deletes the ge-1/1/1 port to bridge br0:

```
admin@Switch$ovs-vsctl del-port br0 ge-1/1/1
```

Controller commands

ovs-vsctl *[--OPTION]* set-controller <*bridge*> <*target*> *[target]*

Set the controllers for <*bridge*>. Support set multiple controllers at same time.
The bridge is typically configured to connect to multiple controllers. The controllers may select a primary controller that takes change of the flow tables of the bridge to inplement a network policy.
The <target> can use any of the following forms:

ovs-vsctl *[--OPTION]* set-controller <*bridge*> tcp:<*ip*>:<*port*>

Connect to controller with tcp port, the default value is 6633.
Example:

```
root@PicOS-OVS$ovs-vsctl set-controller br0 tcp:10.10.50.47:6633
```

ovs-vsctl *[--OPTION]* set-controller <*bridge*> ssl:<*ip*>:<*port*>

Connect to controller with specified SSL port, the default value is 6633.
Example:

```
root@PicOS-OVS$ovs-vsctl set-controller br0 ssl:10.10.50.100:6633
```

ovs-vsctl *[--OPTION]* get-controller <*bridge*>

Print the controllers for <*bridge*>.
Example:

```
ovs-vsctl get-controller br0
```

ovs-vsctl *[--OPTION]* del-controller <*bridge*>

Delete the controllers for <*bridge*>.
Example:

```
ovs-vsctl del-controller br0
```

ovs-vsctl *[--OPTION]* set-fail-mode <*bridge*> <*mode*>

Set the fail-mode for <*bridge*> to <*mode*>.
The <*mode*> used in control flow table when controller failure setting. Support **standalone** and **secure** modes, the default mode is **secure** mode.
If set the mode is standalone, ovs-vswitchd will take over responsibility for setting up flows when connect to controller fail, and all flows in bridge will clear and there is a flow named "normal" to let the switch work as a L2 switch ; If fail-mode set to secure, ovs-vswitchd will not set up flows nor clear all flows. In secure mode, the packet is dropped default, in other word, there is no flow named "normal" to let switch work as a L2 switch
Example:

```
ovs-vsctl set-fail-mode br0 standalone
```

ovs-vsctl *[--OPTION]* get-fail-mode <*bridge*>

Print the fail-mode for <*bridge*>. If not set the fail-mode, will print nothing.
Example:

```
ovs-vsctl get-fail-mode br0
```

ovs-vsctl *[--OPTION]* del-fail-mode <*bridge*>

Delete the fail-mode for <*bridge*>. After delete current mode will return the default mode standalone.
Example:

```
ovs-vsctl del-fail-mode br0
```

Database commands

Database commands create, list and modify the contents of ovsdb tables.PicOS OVS support the following tables, as:

Bridge table

Configure a bridge within an Open vSwitch. Record bridge configurations by _uuid in bridge tables.

Controller table

Configure an OpenFlow controller, record controller infos by _uuid in controller table.

Interface table

Configure a network device attached to a port, record interface configurations by _uuid in interface table.

Mirror table

Configure a mirror port to a bridge, record mirror configurations by _uuid in mirror table.

Open_vSwitch table

The global configurations for ovs-vswitchd, record configurations by _uuid.

Pica8 table

Pica_match_mode table

Port table

Configure bridge ports, record port configurations by _uuid in port table.

QoS table

Configure quality-of-service for a port, record QoS configurations by _uuid in QoS table.

Queue table

Configure one queue within a QoS, record by _uuid in queue table.

SSL table

sFlow table

Configure an sFlow exporter attached to a bridge, record by _uuid in sFlow table.

NetFlow table

Configure a NetFlow attached to a bridge, records by _uuid in NetFlow table.

ovs-vsctl *[--OPTION]* list *<table> [record]*

List the *[record]* record if special *[record]*, otherwise, list all records in *<table>*.
The *[record]* mean _uuid or special name
Examples:

```
admin@XorPlus$ovs-vsctl list port te-1/1/1
_uuid               : e16c6743-999e-49af-8c0a-bc27eb897924
bond_downdelay      : 0
bond_fake_iface     : false
bond_mode           : []
bond_updelay        : 0
external_ids        : {}
fake_bridge         : false
interfaces          : [d8674864-22f1-41eb-8ece-ce35d90c5a64]
lacp                : []
mac                 : []
name                : "te-1/1/1"
other_config        : {}
qos                 : []
statistics          : {}
status              : {}
tag                 : []
trunks              : []
vlan_mode           : []
```

```
admin@XorPlus$ovs-vsctl list bridge
_uuid               : 2fa9c8d9-055e-4c2a-b5e4-2f22505cbda6
```

```
controller          : [07e2aaf5-fca3-4f77-93fe-e726d58637b9]
datapath_id         : "5e3e00e09500169a"
datapath_type       : "pica8"
external_ids        : {}
fail_mode           : []
flood_vlans         : []
flow_tables         : {}
ipfix               : []
lldp_enable         : false
mirrors             : []
name                : "br0"
netflow             : []
other_config        : {}
ports               : [3b4d71fc-eaad-4b01-9b95-be56239f3253, 630fb94c-4a7c-42f7-a195-49fd9f525177, e16c6743-999e-49
protocols           : ["OpenFlow13"]
sflow               : []
status              : {}
stp_enable          : false
```

```
admin@XorPlus$ovs-vsctl list Pica8
_uuid               : 8570c5d9-b22d-40ed-9e84-1c7e3b0e1dfd
combinate_actions_enable: false
cos_map_enable      : true
egress_mode_enable  : false
egress_mode_table   : 0
flow_counter_mode   : []
hardware_type       : "P5401"
l2_l3_buffer_mode   : []
l2_l3_preference    : false
l2_mode_enable      : false
l2_mode_table       : 0
l2gre_key_length    : []
l3_ecmp_max_ports   : 0
l3_mode_enable      : false
l3_mode_table       : 0
lag_advance_hash_mapping_fields: []
loopback_enable     : false
match_mode          : []
port_mode           : max
proxy_arp_subnet    : []
proxy_icmpv6_subnet : []
udf_mode            : []
xovs_crossflow_ports: ["te-1/1/1", "te-1/1/2", "te-1/1/3", "te-1/1/4"]
xovs_openflow_ports : []
xovs_vlans          : ["1", "100-110"]
```

ovs-vsctl *[--OPTION]* find *<table> <condition> [condition…]*

List records satisfying *<condition>* in *<table>*.
The *<condition>* represent a column equels value or not. If the value is specified, the operations can be support: "=", "!=", "<", ">", "<=", ">=", "\{=\}", "\{!=\}", "{<}", "{>}", "{<=}" and "{>=}".
Example:

```
ovs-vsctl find bridge datapath_id=5e3e089e01616580 name=br0
```

ovs-vsctl *[--OPTION]* get *<table> <record > <column> [:key]*

Print values of column in *<record>* in *<table>*. *<table>* mean table name, and *<record>* mean _uuid.
Example:(print the value of datapath_id in the _uuid=80984dfb-5f63-45c8-bd3f-6bda918ffc75 in bridge table.)

```
ovs-vsctl get bridge 80984dfb-5f63-45c8-bd3f-6bda918ffc75 datapath_id
```

ovs-vsctl *[--OPTION]* set *<table> <record > <column> [:key] <=value>*

Set or change the column values in *<record>* in *<table>*.
Example: (change the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl list port ge-1/1/2
```

```
_uuid : 6e7b862a-6503-4f1b-982d-b33b65e3dc01
bond_downdelay : 0
bond_fake_iface : false
bond_mode : []
bond_updelay : 0
external_ids : {}
fake_bridge : false
interfaces : [f1b5568f-bd6f-480d-a9ca-636486f387c2]
lacp : []
mac : []
name : "ge-1/1/2"
other_config : {}
qos : []
statistics : {}
status : {}
tag : 1
trunks : [2000, 4094]
root@PicOS-OVS$ovs-vsctl set port 6e7b862a-6503-4f1b-982d-b33b65e3dc01 trunks=100,200
root@PicOS-OVS$ovs-vsctl list port ge-1/1/2
_uuid : 6e7b862a-6503-4f1b-982d-b33b65e3dc01
bond_downdelay : 0
bond_fake_iface : false
bond_mode : []
bond_updelay : 0
external_ids : {}
fake_bridge : false
interfaces : [f1b5568f-bd6f-480d-a9ca-636486f387c2]
lacp : []
mac : []
name : "ge-1/1/2"
other_config : {}
qos : []
statistics : {}
status : {}
tag : 1
trunks : [100, 200]
vlan_mode : trunk
```

ovs-vsctl *[--OPTION]* destroy *<table> <record>*

Deletes<record> from <table>.

ovs-vsctl *[--OPTION]* add *<table> <record > <column> [key=] <value>*

Add the column values in *<record>* in *<table>.*
Example: (add the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200]
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl add port ge-1/1/2 trunks 100,300
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200, 300]
```

ovs-vsctl *[--OPTION]* remove *<table> <record > <column> [key=] <value>*

Remove the column value in *<record>* in *<table>.*
Example: (remove the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200, 300]
root@PicOS-OVS$ovs-vsctl remove port ge-1/1/2 trunks trunks 100
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[200, 300]
```

ovs-vsctl *[--OPTION]* clear *<table> <record > <column>*

Clear all values from column in <record> in <table>.
Example:
Clear all values of trunks in ge-1/1/2 in port table.

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[200, 300]
root@PicOS-OVS$ovs-vsctl clear port ge-1/1/2 trunks
[]
root@PicOS-OVS$
```

Interface commands

ovs-vsctl *[--OPTION]* list-ifaces *<bridge>*

Print the names of all interfaces on *<bridge>*.
Example:

```
ovs-vsctl list-ifaces br0
```

ovs-vsctl *[--OPTION]* iface-to-br *<interface>*

Print the name of bridge that contains *<port>*.
Example:

```
ovs-vsctl iface-to-br ge-1/1/1
```

Mirror Commands

Chips mirror actions:

PRONTO3290 PRONTO3296 PRONTO3295(TR2)(egress mirror=true)
PRONTO3780 PRONTO3920 PRONTO3922 PRONTO3930 PRONTO3960 PRONTO3965 PRONTO3980 PRONTO3920 PRONTO3924(TD)

ES4654 AS4610_54P AS4610_54T AS4610_30P AS4610_30T(Helix4)(egress mirror=true)
PRONTO5101 PRONTO5401 AS6701_32X N2632XL N2948_6XL AS6712_32X AS5712_54X S4048 ARCTICA4806XP(TD2)

AS5812_54T AS5812_54X(TD2P)
DCS7032Q28 AS7712_32X Z9100 (TH)

Note：Egress mirror works correctly only on those switches that the parameter 'egress mirror' is true.According to above chips,3290（Firebolt3),3296(Triumph2),helix4 support egress mirror.On other switches,the mirror port' traffics' action are not certain.

Below is the test result on some kinds of chips:

p3290(Firebolt3):

module name	**mirror dst traffic test result**
multitable	pass
udf/ttp multicast	pass
push mpls/pop mpls	failed(3290 do not support mpls)
egress mode	pass
flow control	pass
l2mpls	failed(3290 do not support mpls)

p3297(trumph2):

module name	**mirror dst traffic test result**
multitable	pass
ttp multicast	pass
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	mirror test pass
l2mpls	pass

as5812_54t(trident2plus):

module name	**mirror dst traffic test result**
multitable	pass
ttp multicast	failed
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	mirror test pass
l2mpls	failed(mirror port packets has one more vlan 4095)
vxlan/l2gre/NAT	pass

p6701(trident2):

module name	**mirror dst traffic test result**
multitable	pass
ttp multicast	failed
udf/push mpls/pop mpls	pass

egress mode	pass
flow control	pass
l2mpls/nat	pass

vxlan/l2gre	failed

p3920(trident+):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	failed
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	pass
l2mpls	pass

4610_54t_b(helix4):

module name	mirror dst traffic test result
multitable	pass
ttp multicast /udf	pass
push mpls/pop mpls	failed(4610 do not support mpls)
egress mode	pass
flow control	pass
l2mpls	failed(4610 do not support l2mpls)

as7712_32x(tomhark):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	failed
pop mpls/udf	failed(do not support mpls)
egress mode	pass
flow control /l2mpls/nat/push mpls(ip packets)	pass
vxlan/l2gre	failed

Create One Mirror

ovs-vsctl [--OPTION] -- set bridge <bridge> mirrors=@m -- --id=@<port1> get Port <port1> -- --id=@<port2> get Port <port2> [-- --id=@<port3> get Port <port3>]-- --id=@m create Mirror name=<mirror-name> select-src-port=@<port1>[,@<port3>] select-dst-port=@<port1>[,@<port3>] output-port=@<port2>

PicOS OVS supports mirroring, **select-src-port** and **select-dst-port** represent the source ports of mirroring, **select-dst-port** means some packets (in switch chip) will go-out from the specified port (egress); **select-src-port** means some packets will enter the specified port (ingress); **output_port** means the monitor port. PicOS OVS supports up to 4 mirrors.

Before PicOS2.10 ovs only support configure physical port as output_port, from PicOS2.10 ovs also support lag interface as output_port.

Example1:
Add port ge-1/1/1, ge-1/1/2 and ge-1/1/3 to mirror, ge-1/1/1 and ge-1/1/2 as ingress and egress, the output port is ge-1/1/3.

```
root@PicOS-OVS$ovs-vsctl set bridge br0 mirrors=@m -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/2 get Port g
```

Example2:
Add port ge-1/1/1, ge-1/1/2 and ae1 to mirror, ge-1/1/1 and ge-1/1/2 as ingress and egress, the output port is ae1.

```
root@PicOS-OVS$ovs-vsctl set bridge br0 mirrors=@m -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/2 get Port g
```

ovs-vsctl *[--OPTION]* destroy *<table> <record>* – clear Bridge *<bridge>* mirrors

Example:

Delete a mirror named mymirror from mirror table in bridge br0.

```
admin@PicOS-OVS$ ovs-vsctl destroy Mirror mymirror -- clear Bridge br0 mirrors
or
admin@PicOS-OVS$ ovs-vsctl clear Bridge br0 mirrors
```

Create Two Mirrors

```
admin@PicOS-OVS$ovs-vsctl  -- set bridge br-s mirrors=@m,@m1 -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/3
```

Add one mirror and monitor port is lag

```
admin@PicOS-OVS$ovs-vsctl -- add bridge br-s mirrors @m -- --id=@te-1/1/1 get Port te-1/1/1 -- --id=@te-1/1/2 get P
```

Delete one mirror

```
admin@PicOS-OVS$ovs-vsctl remove bridge br0 mirrors 76fd4479-67e9-4c65-8edb-b99d8706d8f9
```

NetFlow Commands

---

ovs-vsctl set Bridge <*bridge*> netflow=@nf -- --id=@nf create NetFlow targets=<*target*> active-timeout=<*timeout*>

Example:

```
admin@PicOS-OVS$ovs-vsctl set Bridge br0 netflow=@nf -- --id=@nf create NetFlow targets=\"10.10.50.207:5566\" activ
In the above CLI, the parametersare shown as following:
COLLECTOR_IP=10.10.50.207
COLLECTOR_PORT=5566
ACTIVE_TIMEOUT=30
```

ovs-vsctl – clear Bridge <*bridge*> netflow

Delete NetFlow from NetFlow table.

Example:
Clear NetFlow from NetFlow table in bridge br0.

```
admin@PicOS-OVS$ovs-vsctl -- clear Bridge br0 netflow
```

Open vSwitch commands

ovs-vsctl init (the command is not effect)

To initialize the Open vSwitch database if not yet initialized. If the database has already been initialized, the init command will have no effect.

ovs-vsctl show

Print a brief overview of database contents.

ovs-vsctl emer-reset

Reset the configurarion to clean state. Using this command can delete fail mode, OpenFLow controllers, port mirrors, NetFlow, sFlow, and IPFIX configuration.

Match-mode Command

ovs-vsctl *[--OPTION]* set-match-mode *<mode:options=priority> [mode:options=priority]*

By default, 2 TCAM entries are used to support all matching tuples for all flows, even if the flow does not use all matching tuples. To optimize the TCAM usage, PicOS-2.1 allows user to configure the switch in short flow TCAM match mode, in which, each flow will only consume 1 TCAM entry. To use this feature, the flow must use the exact fields described below and cannot mix fields from various modes:

When this mode is enabled (with the set-match-mode command), only specific fields can be used in the priority range defined by the command.

From PicOS2.9.0,add a new group(ipv4_quintuple group) for tomahawk platform besides the normal match mode groups supported by other platforms.

The flows must use the exact fields described below:

mac mode: "in_port,dl_src,dl_dst,dl_vlan,dl_type"

ip mode: "in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800"

arp_tpa mode: "in_port, arp_tpa, dl_type=0x0806"

ipv6_full mode: "in_port,dl_vlan,ipv6_src,ipv6_dst,tp_src,tp_dst,nw_proto,dl_type=0x86dd"

ipv6_src mode: "in_port,dl_src,dl_dst,dl_vlan,ipv6_src,nw_proto,dl_type=0x86dd"

ipv6_dst mode: "in_port,dl_src,dl_dst,dl_vlan,ipv6_dst,nw_proto,dl_type=0x86dd"

ipv4_quintuple: "in_port,dl_vlan,nw_src,nw_dst,tp_src,tp_dst,nw_proto,dl_type=0x0800"

For example, if mac mode is enabled, all the flows must only use one or more fields defined in the mac mode. If mac and ip modes are enabled, then you can configure either mac flows or ip flows based on the fields described above. However, you cannot mix the fields from mac and ip (that is, dl_src and nw_src)

Each mode is configured with a priority range that determines the flow priority. The flow priority must be specified when user configures the flow through ovs commands or controller. If user does not want match-mode, configure match-mode as default. The default value is default.

Example:

Configure match-mode mac priority from 200 to 499; ip priority 500-999; arp_tpa priority 1000-2000.

```
root@PicOS-OVS$ovs-vsctl set-match-mode mac=10-1000,ip=2000-20000,arp_tpa=30000-40000,ipv6_full=50000-50001,ipv6_ds
```

Remove match-mode configuration.

```
root@PicOS-OVS$ ovs-vsctl set-match-mode [default]
```

ovs-vsctl show-match-mode

Print current match-mode.

Example:

```
admin@PicOS-OVS$ovs-vsctl show-match-modecurrent match modes:
 ipv4_quintuple:
   priorities={60001-65535}
   fields={in_port,dl_vlan,nw_src,nw_dst,tp_src,tp_dst,nw_proto,dl_type=0x0800}
 ipv6_src:
   priorities={50004-60000}
   fields={in_port,dl_src,dl_dst,dl_vlan,ipv6_src,nw_proto,dl_type=0x86dd}
 ipv6_dst:
   priorities={50002-50003}
   fields={in_port,dl_src,dl_dst,dl_vlan,ipv6_dst,nw_proto,dl_type=0x86dd}
 ipv6_full:
   priorities={50000-50001}
   fields={in_port,dl_vlan,ipv6_src,ipv6_dst,tp_src,tp_dst,nw_proto,dl_type=0x86dd}
 arp_tpa(both):
   priorities={30000-40000}
   fields={in_port,arp_tpa,dl_type=0x0806}
 mac:
   priorities={10-1000}
   fields={in_port,dl_src,dl_dst,dl_vlan,dl_type}
 ip:
   priorities={2000-20000}
   fields={in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800}
```

QoS_queue Commands

ovs-vsctl [--OPTION] -- set port <port> qos=@newqos -- --id=@newqos create qos type=PRONTO_STRICT queues:<queueid>=@newqueue [queues:<queueid>=@newqueue1] -- --id=@newqueue create queue other-config:min-rate=<minrate> other-config:max-rate=<maxrate> [-- --id=@newqueue1 create queue other-config:min-rate=<minrate> other-config:max-rate=<maxrate>]

Queue 0~7 represent priority 0~7, respectively.

Example:
Configure qos contain two queues: queue 0 and queue 7. And min and max rate of queue 0 and queue 7 is set as 10M.

```
admin@PicOS-OVS$ovs-vsctl set port ge-1/1/3 qos=@newqos -- --id=@newqos create qos type=PRONTO_STRICT queues:0=@nev
```

ovs-vsctl *[--OPTION]* clear port <*port*> qos

Delete QoS applied <*port*>.

Example:
Clear QoS and queues applied port ge-1/1/3 from Qos table and queue table.

```
admin@PicOS-OVS$ovs-vsctl clear port ge-1/1/3 qos
admin@PicOS-OVS$ovs-vsctl --all destroy qos
admin@PicOS-OVS$ovs-vsctl --all destroy queue
```

sFlow commands

ovs-vsctl -- --id=@s create sFlow agent=*<agent>* target=*<target>[,<target>,...]* header=*<header>* samping=*<samping>* polling=*<polling>* -- set Bridge *<bridge>* sflow=@s

PicOS OVS supports sFlow v5.
Example:

```
admin@PicOS-OVS$ovs-vsctl -- --id=@s create sFlow agent=eth0 target=\"10.10.50.207:9901\" header=128 sampling=2000
In the above CLI, the parameters are shown as following:
COLLECTOR_IP=10.10.50.207
COLLECTOR_PORT=9901
AGENT_IP=eth0
HEADER_BYTES=128
SAMPLING_N=64
POLLING_SECS=10
```

ovs-vsctl – clear Bridge *<bridge>* sflow

Delete sFlow from sFlow table.
Example:
Clear sFlow from sFlow table in bridge br0.

```
admin@PicOS-OVS$ovs-vsctl -- clear Bridge br0 sflow
```

Troubleshoot the configuration

```
admin@5712$ovs-vsctl list sflow
_uuid               : 3362a543-4a1a-47db-898a-0ec0eddb7aa0
agent               : "eth0"
external_ids        : {}
header              : 128
polling             : 30
sampling            : 2000
targets             : ["172.16.0.173:8008"]
```

Cos-map Command

ovs-vsctl set-cos-map <*TRUE|FALSE*>

From Picos-2.6, user can enable/disable the cos-mapping, the default value is disabled. Once cos-mapping is enabled, the packet with the different cos value is mapped to queue0-7.
Usage:

```
Enable/Disable:
 ovs-vsctl set-cos-map true
 ovs-vsctl set-cos-map false

Set dscp map on port:
 ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2
 equal to:
 ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1 dscp_map:1=q1 dscp_map:2=q2

 Note:
  dscp range is [0, 63];
  queue range value is {q0, q1, q2, q3, q4, q5, q6, q7};
  if a dscp value is not configured, the default queue is q0.

Clear all dscp map on port:
 ovs-vsctl clear interface ge-1/1/1 dscp_map

 Note:
 if no dscp_map configuration, the default map is:

       dscp   queue
    --------  -----
     0 -  7:   q0
     8 - 15:   q1
    16 - 23:   q2
    24 - 31:   q3
    32 - 39:   q4
    40 - 47:   q5
    48 - 55:   q6
    56 - 63:   q7
```

ovs-vsctl show-cos-map

Display the configuration of cos-mapping.
Example:

```
admin@PicOS-OVS$ovs-vsctl show-cos-map
cos mapping: enabled

admin@PicOS-OVS$ovs-vsctl show-cos-map ge-1/1/1
cos mapping: enabled
{
       dscp   queue
    --------  -----
     0 -  7:   q0
     8 - 15:   q1
    16 - 23:   q2
    24 - 31:   q3
    32 - 39:   q4
    40 - 47:   q5
    48 - 55:   q6
    56 - 63:   q7
}
```

Egress-mode Command

ovs-vsctl enable-egress-mode <*TRUE|FALSE*> *[TABLE]*

Enable or disable egress-mode.

If not specified the [TABLE], use table 253 to support another 256 flow, the action of flow should be drop or mod_nw_tos.

eg. The valid table is from 1 to 253, except the table 250, it is used by udf-mode.

> ⚠ egress-mode cannot be configured on the table which has configured L2/L3 mode.

Enable egress-mode on default table or specify table:

```
ovs-vsctl set-egress-mode TRUE
ovs-vsctl set-egress-mode TRUE 251
```

Add flow in egress-mode table:

```
ovs-ofctl add-flow br0 table=253,in_port=1,actions=drop
ovs-ofctl add-flow br0 table=253,dl_type=0x0800,nw_dst=192.168.1.3,actions=mod_nw_tos:16
```

ovs-vsctl show-egress-mode

Show the current configuration of egress-mode.

Set-flow-counter-mode Command

ovs-vsctl set-flow-counter-mode <bytes|packets|both>

Set the flow counter type.

Example:

```
admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode bytes

  Please reboot for the change to take effect!

admin@PicOS-OVS$sudo systemctl restart picos
...............
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is enabled
  Packets mode is disabled

admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=21.563s, table=0, n_packets=n/a, n_bytes=0, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:n/a byte_in_count:0 duration:27.266s bands:
0: packet_count:n/a byte_count:0
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:n/a byte_in_count:151400 duration:33.138s bands:
0: packet_count:n/a byte_count:151400
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=34.288s, table=0, n_packets=n/a, n_bytes=151400, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$

admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode packets

  Please reboot for the change to take effect!

admin@PicOS-OVS$sudo systemctl restart picos
...............
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:n/a duration:12.306s bands:
0: packet_count:0 byte_count:n/a
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is disabled
  Packets mode is enabled

admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:n/a duration:24.705s bands:
0: packet_count:0 byte_count:n/a
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:100 byte_in_count:n/a duration:29.904s bands:
0: packet_count:100 byte_count:n/a
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=38.496s, table=0, n_packets=100, n_bytes=n/a, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$

admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode both

  Please reboot for the change to take effect!
admin@PicOS-OVS$sudo systemctl restart picos

...............
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is enabled
  Packets mode is enabled

admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:0 duration:11.138s bands:
0: packet_count:0 byte_count:0
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=12.808s, table=0, n_packets=0, n_bytes=0, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=18.345s, table=0, n_packets=100, n_bytes=151400, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:100 byte_in_count:151400 duration:24.802s bands:
0: packet_count:100 byte_count:151400
admin@PicOS-OVS$
```

Combinated-mode Command

ovs-vsctl set-combinated-mode <*TRUE|FALSE*>

Enable combinated mode to deal with VCAP/ICAP flow conflict, only half of TCAM flow number can be used.

ovs-vsctl show-combinated-mode

Show whether combinated-mode is enabled or not.

DSCP Commands

DSCP (Differentiated Services Code Point) is a field in the header of an IP packet that is used to provide QoS (Quality of Service). You can mark each packet with a DSCP code and assign to it the corresponding level of service. PicOS 2.6 enables users to map a specific DSCP value to an interface queue. If you do not configure DSCP mappings, PicOS 2.6 uses the following defaults:

DSCP Values	Queue
0-7	q0
8-15	q1
16-23	q2
24-31	q3
32-39	q4
40-47	q5
48-55	q6

The following command is used to enable or disable DSCP mapping:

ovs-vsctl set-cos-map <**true** | **false**>

By default, DSCP mapping is disabled in PicOS 2.6. Once DSCP mapping is enabled, packets with different DSCP values are placed in different queues (q0-q7).

The following example enables DSCP mapping:

ovs-vsctl set-cos-map true

The following example disables DSCP mapping:

ovs-vsctl set-cos-map false

The default DSCP map for interface **ge-1/1/1** can be modified as shown below:

ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2

An alternative method would be to use the following command:

ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1, dscp_map:1=q1 dscp_map:2=q2

DSCP values range from 0 to 63. The available queues are q0, q1, q2, q3, q4, q5, q6, and q7. If a DSCP value is not configured, the default queue is q0. Incoming packets with any DSCP values will be treated the same.

Use the following command to clear the DSCP map of an interface:

ovs-vsctl clear interface ge-1/1/1 dscp_map

Use the following command to set the DSCP map of an interface:

ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2

or

ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1 dscp_map:1=q1 dscp_map:2=q2

You may use the following commands to show the DSCP map:

ovs-vsctl show-cos-map
ovs-vsctl show-cos-map ge-1/1/1

Troubleshooting Guide

- L2/L3 Troubleshooting Guide
- PICOS OVS Troubleshooting
- PICOS System Troubleshooting
- Technical Support
- General PICOS FAQ
- Traceoptions Configuration Commands
- Displaying the Debugging Message

L2/L3 Troubleshooting Guide

This guide describes how to identify and resolve common problems related to the Pica8 PicOS software used on supported switches.

- Monitoring and Debugging L2/L3 protocols
- Routing and Forwarding Table
- Using Pipe (|) Filter Functions
- Using the show tech-support Command

Monitoring and Debugging L2/L3 protocols

Find and Configure the Log File

By default, the syslog local-file is ram. The log file name is "message" which is in the directory "/tmp/log"

```
admin@XorPlus$cd /tmp/log
admin@XorPlus$ls
lastlog lighttpd messages wtmp
```

You can use "tail -f /tmp/log/messages" to display the log messages.

You can set the syslog local-file location to disk. The log file name is "messages" which is in the directory of "/var/log"

```
admin@XorPlus# set system syslog local-file disk
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus$cd /var/log/
admin@XorPlus$ls
apt dmesg fsck last_death lastlog messages news ntpstats wtmp
admin@XorPlus$
```

You can use "tail -f /var/log/messages" to show the log messages.

Enable Important Debugs

Enable debug interface：

```
##Global Interface traceoptions.
admin@XorPlus# set interface traceoptions flag
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all tracing
  config                        Configure configuration tracing
  ethernet-switching-options    Configure ethernet-switching-options tracing
  neighbor-event                Configure neighbor event tracing
  packets                       Configure received or sent packets event tracing
  port-security                 Configure port security tracing
  raw-packet                    Configure receive raw packet tracing
  route-event                   Configure route event tracing
  static-ethernet-switching     Configure static-ethernet-switching tracing
  timer                         Configure timer tracing

admin@XorPlus# set interface traceoptions flag config
  <[Enter]>                     Execute this command
  disable                       Disable configuration tracing

admin@XorPlus# set interface traceoptions flag config disable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set interface traceoptions line-card ?
Possible completions:
  <[Enter]>                     Execute this command
  statistic                     Configure line card statistic module trace
  trace-level                   Configure line card trace level
  trace-type                    Configure line card trace type

admin@XorPlus# set interface traceoptions line-card trace-level all disable false
admin@XorPlus# commit
Commit OK.
```

Enable debug of protocals:

```
admin@Xorplus# set protocols
Possible completions:
  <[Enter]>                     Execute this command
  arp                           Configure ARP
  bgp                           Configure BGP inter-domain routing
  dhcp                          Dynamic Host Configuration Protocol
  dot1x                         802.1x protocol
  igmp                          Configure the IGMP protocol
  igmp-snooping                 Configure the igmp snooping
  lacp                          Link Aggregation Control Protocol
  lldp                          Link Layer Discovery Protocol 802.1AB
  mlag                          Configure MLAG
  neighbour                     Configure Neighbour Discovery Protocol
  netconf                       Configure NETCONF
  ospf                          Configure the OSPF protocol
  ovsdb                         Enable OVSDB
  pim                           PIM protocol
  sflow                         Configure sflow
  snmp                          Simple network management protocol configuration
  spanning-tree                 Configure Spanning Tree
  static                        Configure static routes
  udld                          Unidirectional Link Detection Protocol
  vrrp                          Configure VRRP
```

```
admin@Xorplus# set protocols bgp traceoption updates in
admin@Xorplus# commit
Commit OK
Save Done!
```

Enable debug of LLDP:

```
## LLDP global traceoptions.
admin@Xorplus# set protocols lldp traceoptions flag
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all events and packets tracing
  configuration                 Configure configuration tracing
  message-in                    Configure received message tracing
  message-out                   Configure send message tracing
  state-change                  Configure LLDP state change tracing
admin@Xorplus# set protocols lldp traceoptions flag message-in disable false
admin@XorPlus# commit
Commit OK.
```

Enable debug of LACP:

```
## LACP global traceoptions.
admin@Xorplus# set protocols lacp traceoptions flag
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all events and packets tracing
  configuration                 Configure configuration tracing
  fallback                      Configure FALLBACK tracing
  message-in                    Configure received message tracing
  message-out                   Configure send message tracing
  mlag                          Configure MLAG tracing
  state-change                  Configure LACP state change tracing
admin@Xorplus# set protocols lacp traceoptions flag message-in disable false
admin@XorPlus# commit
Commit OK.


##LACP per interface traceoptions.
admin@Xorplus# set protocols lacp traceoptions interface ge-1/1/1 flag
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all events and packets tracing
  configuration                 Configure configuration tracing
  message-in                    Configure received message tracing
  message-out                   Configure send message tracing
  state-change                  Configure LACP state change tracing
admin@Xorplus# set protocols lacp traceoptions interface ge-1/1/1 flag configuration disable false
admin@XorPlus# commit
Commit OK.
```

Enable debug of UDLD:

```
## UDLD global traceoptions.
admin@Xorplus# set protocols udld traceoptions
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all events and packets tracing
  configuration                 Configure configuration tracing
  event                         Configure event tracing
  packet                        Configure the sending/receiving packets tracing
  raw-packet                    Configure UDLD raw packet tracing
  state-change                  Configure state change tracing
  timer                         Configure UDLD timer tracing
admin@Xorplus# set protocols udld traceoptions event disable false
admin@XorPlus# commit
Commit OK.
```

Enable debug of BGP:

```
admin@XorPlus# set protocols bgp traceoption ?
admin@XorPlus# set protocols bgp traceoption
Possible completions:
  <[Enter]>                     Execute this command
  bestpath                      BGP bestpath
  evpn                          EVPN
  keepalives                    BGP IPv4 neighbor to debug
  neighbor-events               BGP Neighbor Events
  updates                       BGP updates
  zebra                         BGP zebra messages

admin@XorPlus# set protocols bgp traceoption updates in
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Enable debug of ospf:

```
admin@XorPlus# set protocols ospf traceoption ?
Possible completions:
  <[Enter]>                     Execute this command
  ism                           Configure tracing of OSPF interface state machine
  lsa                           Configure tracing of OSPF link state advertisement
  nsm                           Configure tracing of OSPF neighbor state machine
  packet                        Configure tracing of OSPF packets
```

```
  zebra                         Configure tracing of zebra information

admin@XorPlus# set protocols ospf traceoption packet all detail
admin@XorPlus# commit
```

Enable debug of stp:

```
admin@XorPlus# set protocols spanning-tree traceoptions interface ge-1/1/1 ?
Possible completions:
  <[Enter]>                     Execute this command
  all                           Configure all tracing operations
  bridge-detection-machine      Configure bridge detection state machine tracing
  configuration                 Configure configuration tracing
  events                        Configure events tracing
  message-in                    Configure receive message tracing
  message-out                   Configure send message tracing
  mlag                          Configure mlag tracing
  port-information-machine      Configure port information state machine tracing
  port-migration-machine        Configure port migration state machine tracing
  port-receive-machine          Configure port receive state machine tracing
  port-role-selection-machine   Configure port role selection state machine tracing
  port-role-transition-machine  Configure port role transition state machine tracing
  port-state-transition-machine Configure port state transition state machine tracing
  port-transmit-machine         Configure port transmit state machine tracing
  state-machine-variables       Configure state machine variables tracing
  timers                        Configure timers tracing
  topology-change-machine       Configure topology change state machine tracing

admin@XorPlus# set protocols spanning-tree traceoptions interface ge-1/1/1 all disable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Enable debug of igmp:

```
admin@XorPlus# set protocols igmp traceoption ?
Possible completions:
  <[Enter]>                     Execute this command
  events                        IGMP protocol events
  packets                       IGMP protocol packets
  trace                         IGMP internal daemon activity

admin@XorPlus# set protocols igmp traceoption events
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Find the Core Dump File

When the device crashes, it will create a core file which can be found in a directory called *pica/core*.

```
admin@R2:/pica/core$ pwd
/pica/core
```

Find the last_death file for Troubleshooting

You can view the last_death file after the device crashes. It will record the last log message and is located in /var/log directory.

```
admin@R2:/pica/core$ cd /var/log/
admin@R2:/var/log$ ls
btmp   faillog  fsck        lastlog   messages  report_diag.log
dmesg  frr      last death  lighttpd  private   wtmp
```

Routing and Forwarding Table

Check the Software and Hardware Route Tables

To display the hardware *host* route table, use the **show route forward-host ipv4 all** command in L2/L3 operation mode.

```
admin@Switch> show route forward-host ipv4 all
Address HWaddress Port
--------------- ----------------- ---------
10.10.3.2 48:6E:73:02:03:DA ge-1/1/48
Total host count:1
```

To display the hardware route table, use the **show route forward-route ipv4 all** command in L2/L3 operation mode.

```
admin@Switch> show route forward-route ipv4 all
Destination          NextHopMac          Port
---------------      -----------------   ---------
10.10.3.0/24         48:6E:73:02:04:64   connected
101.101.101.0/24     48:6E:73:02:03:DA   ge-1/1/48
102.102.102.0/24     48:6E:73:02:03:DA   ge-1/1/48
Total route count:4
```

To display the software route table, use the **show route ipv4** command in L2/L3 operation mode.

```
admin@Switch> show route ipv4
```

If PicOS is running in OVS mode, check the software and hardware flow tables.

Using Pipe (|) Filter Functions

Pipe (|) Filter Functions

This topic describes the pipe (|) filter functions supported in the Pica8 PicOS L2/L3 CLI (command-line interface). The PicOS L2/L3 mode has a growing number of CLI commands that users can use to troubleshoot common problems. These commands usually generate a lot of output. The use of pipe (|) filter functions increases readability of command output, making troubleshooting more effective.

The following filter functions are available with the PicOS L2/L3:

Function	Description
compare	Compare configuration changes with a prior version
count	Count occurrences
display	Display additional configuration information
except	Show only the lines of output that do not contain a pattern
find	Show output starting from the first occurrence of a pattern
match	Show only the lines of output that contain a pattern
no-more	Disable pagination of command output

Comparing Configurations

The **compare** filter compares the current committed configuration with a previously committed configuration.

```
admin@XorPlus# show | compare rollback nn
```

nn is the index into the list of previously committed configurations, also known as the rollback number. The range of values for **nn** is 01-48.

For example:

```
admin@XorPlus# show | compare rollback 03
```

Counting the Number of Output Lines

To count the number of lines in the output of a command, enter **count** after the pipe symbol (|).

The following example uses **count** with the **show** command in configuration mode to display the number of non-default configuration lines:

```
admin@XorPlus# show | count
Count: 11 lines
```

Displaying Output that Matches a Pattern

To display only the lines of output that match a pattern, enter **match** after the pipe symbol (|).

The following example displays the status of only TbE (terabit Ethernet) interfaces:

```
admin@XorPlus> show interface brief | match te-
te-1/1/1    Enabled     Down    Disabled      Full    Auto
te-1/1/2    Enabled     Down    Disabled      Full    Auto
te-1/1/3    Enabled     Down    Disabled      Full    Auto
te-1/1/4    Enabled     Down    Disabled      Full    Auto
te-1/1/5    Enabled     Down    Disabled      Full    Auto
te-1/1/6    Enabled     Down    Disabled      Full    Auto
te-1/1/7    Enabled     Down    Disabled      Full    Auto
te-1/1/8    Enabled     Down    Disabled      Full    Auto
te-1/1/9    Enabled     Down    Disabled      Full    Auto
te-1/1/10   Enabled     Down    Disabled      Full    Auto
<Some output omitted>
```

Omitting Output that Matches a Pattern

To omit lines from the output of a command that make up a pattern, enter **except** after the pipe symbol (|).

The following example uses **except** with the **show interface brief** command in the operation mode to list the interfaces that are *not* down:

```
admin@XorPlus> show interface brief | except Down
```

Preventing Output from Being Paginated

By default, if the output of a command is longer than the length of terminal screen, user will see the **--More--** message to display the remaining output. Press the space bar to display the remaining output.

User can disable pagination by entering **no-more** after the pipe symbol (|).

The following example displays the output of **show** command, executed in PicOS L2/L3 configuration mode, all at once:

```
admin@XorPlus# show | no-more
```

This feature is useful, for example, when user wants to copy the entire output of a command and paste it into an e-mail to be sent to technical support.

Using the show tech-support Command

Show Tech-Support Command

When contacting Pica8 for technical support, issue the command **show tech-support** because it captures the complete status of a PicOS switch. It is recommended to send the output of **show tech-support** command along with the system log. The following samples describe how to obtain the output.

Log in to the switch and enter the **cli** command at the Linux shell to reach the PicOS L2/L3 operation mode.

```
admin@Leaf-1$cli
Synchronizing configuration...OK.
Pica8 PicOS Version 2.6
Welcome to PicOS L2/L3 on Leaf-1
admin@Leaf-1>
```

Enter the **show tech-support** command.

```
admin@Leaf-1> show tech_support
Start......

Item 1: Display version finished!
Item 2: Display interface finished!
Item 3: Display pica configuration finished!
Item 4: Display system config files finished!
Item 5: Display system process finished!
Item 6: Display fdb table finished!
Item 7: Display fdb entries finished!
Item 8: Display ospf neighbors finished!
Item 9: Display ospf interfaces finished!
Item 10: Display kernel route table finished!
Item 11: Display kernel ipv4 neigh table finished!
Item 12: Display kernel ipv6 neigh table finished!
Item 13: Display kernel neigh vrf finished!
Item 14: Display hard-route table finished!
Item 15: Display system hard-route for host finished!
Item 16: Dispaly system spanning tree interfaces finished!
Item 17: Dispaly spanning tree  bridge finished!
Item 18: Display vlans table finished!
Item 19: Display vlan-interfaces finished!
Item 20: Display core-dump finished!
Item 21: Display system uptime finished!
Item 22: Display arp table!
Item 23: Display neighbor table!
Item 24: Display routes table!
Item 25: Display ipv4 routes in hardware table!
Item 26: Display ipv6 routes in hardware table!
Item 27: Display ipv4 hosts in hardware table!
Item 28: Display ipv6 hosts in hardware table!
Item 29: Display copp statistics!
Item 30: Display mlag domain!
Item 31: Display mlag link!
Item 32: Display mlag config consistency!
Item 33: Display mlag statistic!
Item 34: Display license!
Item 35: Display set!
Item 36: Get error event from log!
Item 37: Display frr configuration finished!
Process BCM commands, total count=47

The information has been stored in /tmp/Leaf-1-201507050614-techSupport.log, please forward to support@pica8.com
```

The last line of the output of **show tech-support** command provides the name and location of the file to which the output was saved. In the above example, the name of the file is *Leaf-1-201507050614-techSupport.log* that has been saved to the */tmp* directory.

You can transfer the file, generated by **show tech-support** command, from the switch to your computer over SCP (Secure Copy Protocol). There is a nice free Windows utility called WinSCP, available for download at https://winscp.net/eng/download.php, which you can use to copy the file from the switch to your computer over SCP.

PICOS OVS Troubleshooting

This section details basic procedures to troubleshoot PicOS switches in OVS (Open vSwitch) mode.

Verifying PicOS Mode

Verify if PicOS is actually running in OVS (Open vSwitch) mode, as described in Checking PicOS Mode.

When PicOS is running in the OVS mode, two processes should be running: **ovsdb-server** and **ovs-vswitchd**.

```
admin@XorPlus$ps -ef | grep ovs
root      1356     1  0 Jan26 ?        00:00:10 /ovs/sbin/ovsdb-server /ovs/ovs-vswitchd.conf.db --pidfile --remote
root      1358     1  0 Jan26 ?        00:19:07 /ovs/sbin/ovs-vswitchd --enable-shared-lcmgr
```

In CrossFlow mode, the router stack must have been initialized in addition to having **ovsdb-server** and **ovs-vswitchd** processes running.

```
admin@XorPlus$ps -ef | grep pica
root     12430     1  0 Jan07 ?        00:05:49 pica_cardmgr
root     12432     1  0 Jan07 ?        01:03:19 pica_sif
root     12439     1  0 Jan07 ?        00:08:45 pica_lacp
root     12441     1 19 Jan07 ?        4-10:50:14 pica_lcmgr
root     12447     1  0 Jan07 ?        00:09:58 pica_login
root     13218     1  0 Jan07 ?        00:20:47 pica_mstp
root     13236     1  0 Jan07 ?        01:25:30 /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/run/xorp_rtrmgr.pi
```

Verifying Bridge Configuration

For the bridge and ports to forward frames in hardware, the **datapath_type** configured for each entity must be set to **pica8**.

```
admin@PicOS-OVS$ovs-vsctl show
ac9e5b1e-4234-4158-9214-5660b9343779
  Bridge east
      Controller "tcp:172.16.0.142:6653"
          is_connected: true
      fail_mode: standalone
      Port "ae1"
          tag: 1
          Interface "ae1"
              type: "pica8_lag"
              options: {lacp-mode=active, lacp-system-priority="32768", lacp-time=slow, lag_type=lacp, link_speed=a
      Port "te-1/1/2"
          tag: 1
          Interface "te-1/1/2"
              type: "pica8"
              options: {flow_ctl=none, link_speed=auto}
      Port "te-1/1/1"
          tag: 1
          Interface "te-1/1/1"
              type: "pica8"
              options: {flow_ctl=none, link_speed=auto}

admin@PicOS-OVS$ovs-ofctl show east
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2): dpid:1deb0ae61be44040
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x4):
 1(te-1/1/1): addr:ff:ff:ff:ff:ff:00
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  10MB-FD 100MB-FD 1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 1000 Mbps now, 10000 Mbps max
 2(te-1/1/2): addr:ff:ff:ff:ff:ff:00
     config:     0
```

```
     state:      LINK_DOWN
     current:    1GB-FD COPPER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  10MB-FD 100MB-FD 1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 1000 Mbps now, 10000 Mbps max
 1025(ae1): addr:ff:ff:ff:ff:ff:00
     config:     0
     state:      LINK_UP
     current:    1GB-FD COPPER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  10MB-FD 100MB-FD 1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 1000 Mbps now, 10000 Mbps max
 LOCAL(east): addr:0a:e6:1b:e4:40:40
     config:     0
     state:      LINK_UP
     current:    10MB-FD COPPER
     supported:  10MB-FD COPPER
     speed: 10 Mbps now, 10 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.4) (xid=0x6): frags=normal miss_send_len=0
admin@PicOS-OVS$
```

Once the ports are configured and verified, flows can be managed in OVS.

Checking Flow Discrepancies

Check **ovs-vswitchd** flow discrepancies between the control plane and hardware:

```
admin@PicOS-OVS$ovs-ofctl dump-tables br0 | grep -v active=0:
  0: active=4, lookup=n/a, matched=n/a

admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=1449.903s, table=0, n_packets=n/a, n_bytes=0, in_port=1,dl_src=00:00:3d:a6:c8:f2 actions=outp
 cookie=0x0, duration=1444.537s, table=0, n_packets=n/a, n_bytes=0, in_port=1,dl_src=00:00:3d:a6:c9:14 actions=outp
 cookie=0x0, duration=71723.842s, table=0, n_packets=n/a, n_bytes=0, mpls,in_port=1,dl_vlan=1,mpls_label=10 actions
 cookie=0x0, duration=74839.581s, table=0, n_packets=n/a, n_bytes=923443200, in_port=1 actions=output:2
```

Display hardware flows as shown below:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#24 normal permanent priority=32769,in_port=1,dl_src=00:00:3d:a6:c8:f2, actions:2
#23 normal permanent priority=32769,in_port=1,dl_src=00:00:3d:a6:c9:14, actions:1
#22 normal permanent priority=32769,mpls,in_port=1,dl_vlan=1,mpls_label=10, actions:3
#21 normal permanent priority=32769,in_port=1, actions:2
#20 normal permanent priority=0, actions:drop
Total 5 flows in HW.
```

Displaying OVSDB

Display the full OVSDB (Open vSwitch Database) as shown below:

```
admin@Leaf1$ovsdb-client dump
Bridge table
_uuid                                controller                                datapath_id        datapath_type extern
------------------------------------ ----------------------------------------- ------------------ ------------- ------
c880536a-b614-41bf-9870-2d0bdab3664f [bedb4af7-2125-4346-8c89-bf61bd21f63b] "4c3e486e730203da" "pica8"       {}
<Some output omitted>
```

Debug Packet-In Messages

To debug the protocol messages between the switch and the controller, use the **ovs-ofctl snoop** command in the OVS mode. The following commands debug the protocol messages exchanged between the **br0** bridge and the controller:

```
admin@Switch$ovs-ofctl snoop br0
```

Debug while switch port cannot up

Issue 1, During add port error.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 te-1/1/49 vlan_mode=trunk tag=1 -- set i
nterface te-1/1/49 type=pica8
ovs-vsctl: Error detected while setting up 'te-1/1/49'.  See ovs-vswitchd log for details.
admin@PicOS-OVS$
```

Please check license installed or not.

```
admin@PicOS-OVS$license -s
```

If no license installed, please install license first; If license has installed but the port also add error, please check the port whether is valid in the switch.

```
admin@PicOS-OVS$ovs-appctl pica/show
```

Issue 2, Port cannot up.

```
admin@PicOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2):
dpid:0x5e3e047d7b6293ff(6790870225108767743)
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
 1(te-1/1/1): addr:04:7d:7b:62:93:ff
     config:     0
     state:      LINK_DOWN
     current:    FIBER
     advertised: 1GB-FD 10GB-FD FIBER
     supported:  1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 0 Mbps now, 10000 Mbps max
```

1, Please verify the connection, make sure the connect is correct.

2, Use CLI check module plugin or not.

```
admin@PicOS-OVS$ovs-invctl enable-sfp true
admin@PicOS-OVS$ovs-invctl show-sfp-qsfp
```

3, If there is no module informations about the port, please repeat plugin module to check log messages.

```
admin@PicOS-OVS$ovs-appctl vlog/set hwlog
admin@PicOS-OVS$ovs-appctl hwlog/set-type config true
admin@PicOS-OVS$ovs-appctl hwlog/set-level all debug

Jan  5 2017 14:32:41 XorPlus daemon.warning : 14:32:41.220|ovs|00009|pica private|WARN|SFP te-1/1/1 is plugged in, optical module t
```

4, If there is no log message as above. This is bug, please contract us.

5, If there have log message, and can read module use cammand 'ovs-invctl show-sfp-qsfp'. But port still cannot up, this also one bug, please contract us.

```
ec869713-92af-406e-abb4-f60efdec59f3
  port_name: "te-1/1/1"
  vendor_name: OEM
  vendor_sn: "A85351050280"
  wavelength: "850 nm"
  temperature: "82 F"
  supply_voltage: "3.00 V"
  connector: LC
  length_copper: "0 m"
  length_50m: "80 m"
  length_625m: "20 m"
  length_9m: "300 m"
  length_9m_km: "0 m"
  plugged_in: true
  rx_receive_power: "-2.68 dbM"
  tx_bias_current: "6.00 mA"
  tx_optical_power: "-3.26 dbM"
```

6, If there have plug-in log message, but the module is unknown. Like below.

```
Jan  5 2017 14:41:14 XorPlus daemon.warning : 14:41:14.631|ovs|00014|pica_private|WARN|SFP te-1/1/1 is plugged in, optical module t

admin@PicOS-OVS$ovs-invctl show-sfp-qsfp
d664a803-a6a1-4582-b162-6b9e617df2ea
  port_name: "te-1/1/1"
  vendor_name: FINISAR
  vendor_sn: "P117EWY"
  wavelength: "850 nm"
  temperature: "117995 F"
  supply_voltage: "65535.00 V"
  connector: LC
  length_copper: "0 m"
  length_50m: "300 m"
  length_625m: "150 m"
  length_9m: "0 m"
  length_9m_km: "0 m"
  plugged_in: true
  rx_receive_power: "65535.00 dbM"
  tx_bias_current: "65535.00 mA"
  tx_optical_power: "65535.00 dbM"
```

7, Please check the speed of module is same as the max speed of port supported. If it is, this is a bug, please contract us;

If the speed of module less than the max speed of port, please configure the port speed as the module. If the port also cannot up this time, please contract us.

```
admin@PicOS-OVS$ovs-vsctl set interface te-1/1/1 options:link_speed=1G

admin@PicOS-OVS$ovs-ofctl show br0
OFPT_FEATURES_REPLY (OF1.4) (xid=0x2):
dpid:0x5e3e047d7b6293ff(6790870225108767743)
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
OFPST_PORT_DESC reply (OF1.4) (xid=0x3):
 1(te-1/1/1): addr:04:7d:7b:62:93:ff
     config:     0
     state:      LINK_UP
     current:    1GB-FD FIBER
     advertised: 1GB-FD FIBER
     supported:  1GB-FD 10GB-FD FIBER AUTO_NEG
     speed: 1000 Mbps now, 10000 Mbps max
```

PICOS System Troubleshooting

User can troubleshoot by checking system logs and PIcOS works mode.

- Reset the Switch to Factory Default
- Automating Ping to Multiple Hosts
- Troubleshooting Switch Crashes
- CPU/Memory Rate Limit
- High CPU Utilization
- Backup Partition for PicOS
- SSH Server Preparation
- Linux_configure.py script
- Provision.py script
- How to Disable Weak SSH Cipher/ MAC Algorithms in PICOS

Check log using two methods as follows:

> **NOTE:**
> Users should not put their other files in the /tmp directory, because the space size limit of the /tmp directory is 50M, once exceeded, it will lead to unpredictable system errors.

System logs are stored in two locations:

```
/var/log/messages
```

This directory is stored in Flash.

and

```
/tmp/log/messages
```

This directory is stored in RAM.

Switches use flash memory that has a limited number of lifetime write operations. Hence, it is important that logs are not written continuously to the flash memory. This would dramatically impact the lifetime of the flash memory.

This is why most of the log information is written by default on the /tmp directory.

```
admin@XorPlus$df
Filesystem     1K-blocks   Used Available Use% Mounted on
rootfs           6202636 900184   4987368  16% /
/dev/root        6202636 900184   4987368  16% /
tmpfs             207348     28    207320   1% /run
tmpfs               5120      0      5120   0% /run/lock
tmpfs             414680      0    414680   0% /run/shm
tmpfs              51200     36     51164   1% /tmp
```

The "/tmp" directory is mounted on "tmpfs" which is a filesystem mounted in RAM.

The tmp logs are moved to /var/log when dramatic events occur like system crash or system reboot.

Checking PicOS works mode as follows:

In L2/L3 Mode (Or XORP), only the XORP system is running.

```
admin@PicOS-OVS$ps aux | grep ovs | grep -v grep
admin@PicOS-OVS$
admin@XorPlus$ps aux | grep xorp | grep -v grep
root 16383 0.0 1.2 18100 6596 ? S Jan29 5:26 xorp_policy
root 16385 0.3 2.5 34980 13380 ? Ss Jan29 99:20 /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/run/xorp_rtrmgr.pi
```

In OVS Mode, only the OVS daemon is running.

```
admin@PicOS-OVS$ps aux | grep xorp | grep -v grep
admin@PicOS-OVS$
admin@PicOS-OVS$ps aux | grep ovs | grep -v grep
root 1984 0.0 0.1 6696 2524 ? S Nov13 0:10 ovsdb-server /ovs/ovs-vswitchd.conf.db --pidfile --remote=ptcp:6640:10.
```

```
root 1989 25.6 1.5 113256 32392 ? Sl Nov13 1393:50 ovs-vswitchd --pidfile=ovs-vswitchd.pid --overwrite-pidfile
```

Reset the Switch to Factory Default

Occasionally, it could be useful to reset the equipment to factory default (to erase all configurations or tools on the equipment).

This can be done using the Upgrade command and an image of PicOS, for details about the usage of Upgrade command, please see Upgrading PICOS from Version 4.0.0 or Later Using Upgrade Command.

Here is an example:

```
admin@XorPlus$sudo upgrade picos-2.4-P3295-13912.tar.gz factory-default
```

Automating Ping to Multiple Hosts

PicOS switches support **ping**, which may be used to test connectivity to remote IP addresses. Users often want to test connectivity to all subnets in their network. This can be accomplished manually by pinging IP addresses in all subnets one-by-one, but that method is error-prone and tedious.

This section describes how to write a simple re-usable script to ping a number of IP addresses at once. This script is especially useful when troubleshooting connectivity in a network, and user needs to ping a number of IP addresses again and again for verification.

User can create the script once and use it again and again from the PicOS L2/L3 operation mode.

This requires a text editor to create the script and save it as a file on user's PicOS switch. PicOS includes the **vi** text editor, which can be run from the Linux shell on user's PicOS switch. We choose to call our script **pingAll.sh** though user may choose any other name. The **.sh** file extension is not mandatory, though we recommend using it to make it obvious to anyone that the file is a shell script.

```
admin@Leaf-1$vi pingAll.sh
```

Inside the **vi** editor, press **i** to be able to insert text. Paste the following lines of text (after modifying them for user's network):

```
ip[0]='192.168.42.2'
ip[1]='192.168.42.4'
ip[2]='192.168.42.5'
ip[3]='192.168.42.9'
ip[4]='192.168.42.20'
ip[5]='192.168.42.40'
ip[6]='192.168.42.60'
ip[7]='192.168.42.100'
ip[8]='192.168.42.110'
ip[9]='192.168.42.120'
ip[10]='192.168.42.130'
ip[11]='192.168.42.240'
ip[12]='192.168.42.22'

for ((i=0; i <=12; i++))
do
   ping -c 3 ${ip[$i]}
done
```

Press **Esc** and then enter **:wq** to save the file and exit the **vi** editor.

Some information about the script follows. The **ip[]** array has thirteen elements (**ip[0]** – **ip[12]**) and each element holds an IP address. User can change both the IP addresses and the number of array elements. The script will send three ping requests to each IP address in the **ip[]** array, one by one. If user is familiar with shell scripting or programming in C-like languages, the script should be self-descriptive. Even if user is an absolute beginner to programming and scripting, user should be able to modify and use the script after some research.

List the contents of user's home directory.

```
admin@Leaf-1$ls
pingAll.sh
```

Make the new file **pingAll.sh** executable.

```
admin@Leaf-1$chmod +x pingAll.sh
```

Enter the PicOS L2/L3 operation mode.

```
admin@Leaf-1$cli
Synchronizing configuration...OK.
Pica8 PicOS Version 2.6
Welcome to PicOS L2/L3 on Leaf-1
admin@Leaf-1>
```

Run the script from PicOS L2/L3 operation mode.

```
admin@Leaf-1> bash /home/admin/pingAll.sh
PING 192.168.42.2 (192.168.42.2) 56(84) bytes of data.
64 bytes from 192.168.42.2: icmp_req=1 ttl=64 time=4.66 ms
64 bytes from 192.168.42.2: icmp_req=2 ttl=64 time=0.848 ms
64 bytes from 192.168.42.2: icmp_req=3 ttl=64 time=0.910 ms

--- 192.168.42.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.848/2.142/4.669/1.787 ms
PING 192.168.42.4 (192.168.42.4) 56(84) bytes of data.
64 bytes from 192.168.42.4: icmp_req=1 ttl=64 time=8.27 ms
64 bytes from 192.168.42.4: icmp_req=2 ttl=64 time=1.98 ms
64 bytes from 192.168.42.4: icmp_req=3 ttl=64 time=2.94 ms

--- 192.168.42.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.986/4.401/8.273/2.765 ms
PING 192.168.42.5 (192.168.42.5) 56(84) bytes of data.
64 bytes from 192.168.42.5: icmp_req=1 ttl=64 time=6.59 ms
64 bytes from 192.168.42.5: icmp_req=2 ttl=64 time=3.22 ms
64 bytes from 192.168.42.5: icmp_req=3 ttl=64 time=1.81 ms

--- 192.168.42.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.812/3.876/6.594/2.006 ms

<Some output omitted>
```

Troubleshooting Switch Crashes

The PicOS switch may restart after detecting an unrecoverable error. This situation is usually referred to as a *system crash*.

When the switch crashes, it will create a core file that user can use to figure out what went wrong. The core file is stored in the directory */pica/core*. Use the **file list** command in PicOS L2/L3 operation mode to display the contents of the directory.

```
admin@LEAF-A> file list /pica/core
total 0
```

The output above shows that there is no file in the /pica/core directory. The switch we used never crashed and did not create any core file.

The PicOS writes the last log messages to the */var/log/last_death* file after a system crash.

```
admin@LEAF-A> file show /var/log/last_death | count
Count: 405 lines
admin@LEAF-A> file show /var/log/last_death | match lcmgr
Jun 23 2015 04:08:56 XorPlus local0.info : [PICA_MONITOR]Process pica_lcmgr, running, PID 2823
Jun 23 2015 04:08:56 XorPlus local0.info : [PICA_MONITOR]Monitor for process pica_lcmgr started
Jun 23 2015 04:44:32 XorPlus local0.err : [LCMGR]Someone set counter interval to ZERO!!
Jun 23 2015 04:44:34 XorPlus local0.err : [RTRMGR]XRL Death: class lcmgr01 instance lcmgr01-5eeea3b7d435a0b7277ba87
time:Thu Jan 1 00:43:34 1970 death module:lcmgr01
```

CPU/Memory Rate Limit

From PicOS 2.6, we added the CPU rate limit for processes of PicOS. Including pica_lcmgr, pica_sif, and ovs-vswitchd.

Summary:

- The default CPU usage is 40% if not provided, and default memory size is 150 MB.
- The warning message will be printed if the memory size is bigger than the default value.
- The CPU limitation is based on all CPU's on the system. If the system CPU is P2020 dual cores, 40% CPU limitation is equal to 80% single CPU.

Running CPU/memory rate limit tools manually as follows:

```
sudo /pica/bin/system/tools/pica_monitor -v -c 40 -m 150 pica_lcmgr
```

Checking CPU/memory rate limit tools as follows:

```
admin@XorPlus$ps -aux | grep pica_monitor
warning: bad ps syntax, perhaps a bogus '-'?
See http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ
root      3420  0.6  0.7  38944  3896 ?        S<l  Apr07   3:42 /pica/bin/system/tools/pica_monitor -c 40 -m 150 p
admin    26490  0.0  0.1   2128   688 pts/0    S+   03:26   0:00 grep --color=auto pica_monitor
admin@XorPlus$
```

High CPU Utilization

CPU (Central Processing Unit) utilization is the percentage of time the CPU spends on processing, as compared to the time it sits idle.

The Pica8 PicOS switches will start to experience problems if the CPU utilization begins to reach 75%. User doesn't have to be concerned about brief periods of high CPU utilization. However, if CPU utilization remains consistently high, user needs to investigate further.

The symptoms include:

- Poor system performance
- Switch management slower than usual
- Ping to the management interface times out
- Packet drops

Step 1

To diagnose why a PicOS switch is slow, start with the **top** command. By default, **top** runs in interactive mode and updates its output every few seconds.

```
admin@Switch$top
top - 22:02:10 up 40 days, 13:06,  1 user,  load average: 0.01, 0.02, 0.00
Tasks:  61 total,   2 running,  59 sleeping,   0 stopped,   0 zombie
%Cpu(s):  4.5 us,  0.5 sy,  0.0 ni, 94.5 id,  0.0 wa,  0.0 hi,  0.5 si,  0.0 st
KiB Mem:   2073452 total,   243996 used,  1829456 free,    10728 buffers
KiB Swap:        0 total,        0 used,        0 free,   106620 cached
  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM     TIME+ COMMAND
 6089 root      40   0  128m  31m  13m S   8.6  1.6 576:55.72 pica_lcmgr
 6986 root      40   0 65456  27m 4144 S   1.3  1.3  30:18.82 xorp_rtrmgr
 6080 root      40   0 44156  22m  11m R   0.7  1.1  18:38.42 pica_sif
 7075 root       9 -11 41412 3980 3464 S   0.7  0.2  51:39.71 pica_monitor
    1 root      40   0  2520  852  736 S   0.0  0.0   7:35.99 init
    2 root      40   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      rt   0     0    0    0 S   0.0  0.0   0:01.73 migration/0
    4 root      20   0     0    0    0 S   0.0  0.0   0:04.61 ksoftirqd/0
    5 root      rt   0     0    0    0 S   0.0  0.0   0:02.29 migration/1
    6 root      20   0     0    0    0 S   0.0  0.0   0:06.39 ksoftirqd/1
    7 root      20   0     0    0    0 S   0.0  0.0   0:06.47 events/0
    8 root      20   0     0    0    0 S   0.0  0.0   0:00.14 events/1
    9 root      20   0     0    0    0 S   0.0  0.0   0:00.07 khelper
   13 root      20   0     0    0    0 S   0.0  0.0   0:00.00 async/mgr
  134 root      20   0     0    0    0 S   0.0  0.0   0:00.02 sync_supers
  136 root      20   0     0    0    0 S   0.0  0.0   0:00.20 bdi-default
  137 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kblockd/0
  138 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kblockd/1
  144 root      20   0     0    0    0 S   0.0  0.0   0:00.00 ata/0
```

CPU-bound load is caused when too many processes contend for CPU resources. To check whether load is CPU-bound, check the third line of output:

```
%Cpu(s):  4.5 us,  0.5 sy,  0.0 ni, 94.5 id,  0.0 wa,  0.0 hi,  0.5 si,  0.0 st
```

Each of the percentages indicates the fraction of CPU time consumed by a category of tasks. Symbol **us** indicates the CPU usage of user processes, and **sy** indicates the CPU usage of the kernel and other system processes. CPU-bound load should result in a high percentage of either **us** (user) or **sy** (system) CPU time.

If the user or system percentage is high, the load is likely to be CPU-bound. To narrow down the root cause, look at the processes that consume the highest percentage of CPU resources. By default, **top** sorts processes based on the percentage of CPU usage, with the top consumers appearing first. Once user is armed with the knowledge of processes with the highest CPU utilization, further troubleshooting can be done.

Step 2

Check the log messages for any errors or warning for the following important PicOS modules:

PicOS L2/L3 Mode: pica_lcmgr, pica_sif, and xorp_rtrmgr

PicOS OVS Mode: ovs-vswitchd, and ovsdb-server

By default, the log file is **/tmp/log/messages**. The file may be huge with possibly several thousand lines. Examine the log file using the **cat** command, with an appropriate pipe (|) filter function:

```
admin@Switch$cat /tmp/log/messages | grep lcmgr
Aug 29 2015 01:30:57 SPINE-B local0.info : [PICA_MONITOR]Process pica_lcmgr, running, PID 12983
Aug 29 2015 01:30:57 SPINE-B local0.info : [PICA_MONITOR]Monitor for process pica_lcmgr started
Sep  1 2015 18:07:00 SPINE-B local0.warning : [PICA_MONITOR]pica_lcmgr cpu rate limit 0.80, cpu 0.81 working-rate (
```

```
Sep  3 2015 13:13:32 XorPlus local0.err : [RTRMGR]XRL Death: class lcmgr01 instance lcmgr01-87510959a54d13e97bb845
Sep  3 2015 13:14:28 XorPlus local0.info : [PICA_MONITOR]Process pica_lcmgr, running, PID 23228
Sep  3 2015 13:14:28 XorPlus local0.info : [PICA_MONITOR]Monitor for process pica_lcmgr started
Sep  7 2015 05:05:10 SPINE-B local0.warning : [PICA_MONITOR]pica_lcmgr cpu rate limit 0.80, cpu 0.80 working-rate
Sep 11 2015 05:37:12 SPINE-B daemon.notice : 05:37:12.480|ovs|00001|lcmgr_shared|INFO|XOVS got system mac (48:6e:7
Sep 11 2015 05:37:12 SPINE-B daemon.notice : 05:37:12.481|ovs|00002|lcmgr_shared|INFO|XOVS got QE port mode (0)
Sep 11 2015 05:37:12 SPINE-B daemon.notice : 05:37:12.481|ovs|00003|lcmgr_shared|INFO|XOVS got flow count limitati
Sep 11 2015 05:37:12 SPINE-B daemon.notice : 05:37:12.492|ovs|00001|lcmgr_shared(sif_handler1)|INFO|sif handler cr

<Some output omitted>
```

Step 3

Check the core dump in the */pica/core* directory.

Step 4

To display the virtual interfaces configured on the switch, use the **ifconfig** command at the Linux shell:

```
 admin@Switch$ifconfig
eth0      Link encap:Ethernet  HWaddr 48:6e:73:02:04:63
          inet addr:192.168.42.110  Bcast:192.168.42.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2379952 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1060135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:354374731 (337.9 MiB)  TX bytes:152816006 (145.7 MiB)
          Base address:0x2000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:98303973 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98303973 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:860429061 (820.5 MiB)  TX bytes:860429061 (820.5 MiB)
vlan.3    Link encap:Ethernet  HWaddr 48:6e:73:02:04:64
          inet addr:10.10.3.1  Bcast:10.10.3.255  Mask:255.255.255.0
          inet6 addr: fe80::4a6e:73ff:302:464/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36973 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:2927602 (2.7 MiB)  TX bytes:2743024 (2.6 MiB)
```

Step 5

To display packets on a specific virtual interface, use the **tcpdump** command at the Linux shell:

```
admin@Switch$sudo tcpdump -i vlan.3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan.3, link-type EN10MB (Ethernet), capture size 65535 bytes
```

To debug the protocol messages between the switch and the controller, use the **ovs-ofctl snoop** command in the OVS mode. The following commands debug the protocol messages exchanged between the **br0** bridge and the controller:

```
admin@Switch$ovs-ofctl snoop br0
```

Common Causes

In the CrossFlow mode, both L2/L3 and OVS processes are running. The switch has to process both OVS protocol messages and the L2/L3 packets like BPDUs, OSPF packets, and BGP packets. The switch is likely to have a higher CPU utilization in the CrossFlow mode compared with the L2/L3 or OVS modes.

Normally, the CPU-bound packets are less than 1000 pps (packets per second), and the CPU utilization is not high. However, the **eth0** management interface has no rate limiting configured. Therefore, an attacker can send a large number of packets to the management interface, making the switch slow and even unusable for legitimate traffic.

Possible Fixes

User can deploy the following fixes for high CPU utilization:

1. Add a default drop flow for table-miss packets, to prevent these packet from causing high CPU utilization.
2. Remove some flows with actions: *Controller*, *LOCAL*
3. Make sure that the controller is not sending exessive OpenFlow messages to the switch.
4. Configure the management interface **eth0** at a low speed like 10 Mbps, using the **ethtool -s eth0 speed 10** command.
5. Reload the switch

Backup Partition for PicOS

Backup partition for PicOS:

PowerPc Platform:
We use backup partitions for PicOS to upgrade the system and recover PicOS. Usually users need to reserve about 400 MB for partition 2(eg:sda2). The rest of the SD card belongs to partition 1(eg：sda1). If the size of the SD card is 2 GB, partition 1 should be 1.6GB (1600M) and partition 2 is 400M.

```
Command (m for help): p
Disk /dev/sda: 8004 MB, 8004304896 bytes
247 heads, 62 sectors/track, 1020 cylinders, total 15633408 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
Device Boot Start End Blocks Id System
/dev/sda1 62 12603421 6301680 83 Linux             ------the primary partition for PicOS
/dev/sda2 12603422 15620279 1508429 83 Linux         ------the backup partition for PicOS
```

X86 platform:
There are two partitioning ways used with ONIE, GPT and MBR. With GPT partitioning, the sda1/2MB, is allocated to GRUB as BOOT PARTITION. The second partition is used by ONIE itself. The 3rd or others are free, and can be used by NOS. In this mode, the 3rd partition is allocated to PICOS GRUB, for the grub bootup config files. 4th and 5th are for PicOS and PicOS-BACKUP. When the user runs uninstall from ONIE, all partitions except 1st and 2nd are reserved, all NOS are wiped out. With MBR partitioning mode (which is not recommended), the GRUB boot codes are saved before MBR sector and first partition, the first partition is used by ONIE itself. PicOS begins from the 2nd partition for PicOS-GRUB, PicOS and PicOS-BACKUP partitions.

eg:(With MBR)

```
/dev/sda1: LABEL="ONIE-BOOT" UUID="08ae2c6a-6f14-498f-8e13-d0e7c0a567c1"
/dev/sda3: LABEL="PicOS" UUID="b2735e76-8594-41b9-87e7-d25113dc22f7"        ------the primary partition for PicOS
/dev/sda2: LABEL="PICOS-GRUB" UUID="ca79674b-70fc-4540-b9ef-c98c3afadce3"
/dev/sda4: LABEL="PICOS-BAK" UUID="92028225-403a-44d4-a40e-25e26d46373b"     ------the backup partition for PicOS
```

eg:(with GPT)

```
Disk /dev/sda: 15649200 sectors, 7.5 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 1687245E-B39A-48E5-860B-D7967A67FBE8
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 15649166
Partitions will be aligned on 1-sector boundaries
Total free space is 8547665 sectors (4.1 GiB)
Number Start (sector) End (sector) Size Code Name
1 2048 6143 2.0 MiB EF02 GRUB-BOOT
2 6144 268287 128.0 MiB 3000 ONIE-BOOT
3 268288 1244140 476.5 MiB 0700 PICOS-GRUB
4 1244141 5150390 1.9 GiB 0700 PicOS            -----the primary partition for PicOS
5 5150391 7103515 953.7 MiB 0700 PICOS-BAK       ------the backup partition for PicOS
```

SSH Server Preparation

Add the PKI files、two scripts and the PicOS image on the ssh server.

1: The directory of ssl-private-key (Our openssl connection is not ready, so you only need to create these key files on the server)

```
root@dev-1:/ssl#ls
cacert.pem  sc-cert.pem  sc-privkey.pem
```

Linux_configure.py script

This script usually starts automatically at the end of the configuration interactive shell. This script can set hostname, create accounts and update the time via ntp. You can modify or add this script to define the hostname and accounts and passwords.

```
root@dev-1:/pica8# vim linux_configure.py
 _hostname = "HostName-Test"
_accounts = {"lily":"1R.O.4HRDfvEY", "tom":"7hCft0situjJQ"}
```

> The password of the user should be created by password generator.

Provision.py script

This script usually starts automatically at the end of configuration interactive shell. It is used to download PKI files、PicOS image and linux_configure.py, and then for updating the image and running the linxu_configure.py. You should modify the scipt to define the directory of the files.

```
root@dev-1:/pica8# vim provision.py
 _server_paths = {
     "pki_sw_pri_key":"/ssl/sc-privkey.pem",
     "pki_sw_ca":"/ssl/sc-cert.pem",
     "pki_ctl_ca":"/ssl/cacert.pem",
     "ovs_upgrade_deb":"/pica8/pica-ovs-2.5-P3290-17741.deb",
      "linux_configure_script":"/pica8/linux_configure.py"
}
```

How to Disable Weak SSH Cipher/ MAC Algorithms in PICOS

Requirement

Some of the security scans may show below Server-to-Client or Client-To-server encryption algorithms as vulnerable:
arcfour
arcfour128
arcfour256

Below are some of the Message Authentication Code (MAC) algorithms:
hmac-md5
hmac-md5-96
hmac-sha1-96

> **NOTE:**
> PICOS 3.1.0 and the later version use OpenSSH(?) version is 6.7p1 and following are default Ciphers:
>
> chacha20-poly1305@openssh.com,
>
> aes128-ctr,aes192-ctr,aes256-ctr,
>
> aes128-gcm@openssh.com,aes256-gcm@openssh.com

Description

Verify weak cipher and MAC algorithms are currently used by the SSH running in PICOS switch.

Perform following three steps:

1. First check the cipher and MAC algorithms currently supported in the PICOS SSH protocol.

Check the version of SSH:

```
root@Xorplus:/etc/ssh# ssh -v

OpenSSH_6.0p1 Debian-4+deb7u2, OpenSSL 1.0.1e 11 Feb 2013
```

2. Check what cipher and MAC algorithms are currently supported.

From another Linux Server run the following to list the cipher and MAC algorithms supported by PICOS, using the following command:
nmap --script ssh2-enum-algos -sV -p 22 <IP of PICOS switch>

Example output:

```
root@AutomationServer1 html]# nmap --script ssh2-enum-algos -sV -p 22 172.16.0.191


Starting Nmap 6.40 ( http://nmap.org ) at 2019-03-14 14:13 PDT

Nmap scan report for 172.16.0.191

Host is up (0.00079s latency).

PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 6.0p1 (protocol 2.0)

| ssh2-enum-algos:

|   kex_algorithms (7)

|       ecdh-sha2-nistp256

|       ecdh-sha2-nistp384

|       ecdh-sha2-nistp521

|       diffie-hellman-group-exchange-sha256
```

```
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms (3)
|       ssh-rsa
|       ssh-dss
|       ecdsa-sha2-nistp256
|   encryption_algorithms (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
|       aes256-cbc
|       arcfour
|       rijndael-cbc@lysator.liu.se
|   mac_algorithms (11)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-sha2-256
|       hmac-sha2-256-96
|       hmac-sha2-512
|       hmac-sha2-512-96
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
```

3. From the above output decide which cipher or MAC algorithm you want to disable. For example say you want to disable arcfour cipher algorithm.

Solution

Disable weak Cipher and MAC algorithms used by the SSH running in PICOS switch by performing the following three steps:

1. Disable the weak Cipher and MAC algorithms used by the SSH running in PICOS switch as follows:

You could disable the Ciphers using the command below:

```
# vi /etc/ssh/sshd_config

Press key 'i' to insert and copy the lines below to the end of the file (put only the cipher and MAC algorithms tha

Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,aes192-cbc,aes256-cbc

Macs hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512
```

Save the file.

2. On the PICOS switch restart SSH with the following Linux command:

```
/etc/init.d/ssh restart
```

3. Verify whether weak Cipher and MAC algorithms are now not used by the SSH running in PICOS switch:

From another Linux Server run the following to list the cipher and MAC algorithms supported by PICOS, using the following command:
nmap --script ssh2-enum-algos -sV -p 22 <IP of PICOS switch>

You will see arcfour cipher algorithm is not used by SSH from the following output.

This would show the only the allowed cipher and MAC algorithms now.

Example output:

```
root@AutomationServer1 html]# nmap --script ssh2-enum-algos -sV -p 22 172.16.0.191

Starting Nmap 6.40 ( http://nmap.org ) at 2019-03-14 14:35 PDT

Nmap scan report for 172.16.0.191

Host is up (0.00055s latency).

PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 6.0p1 (protocol 2.0)

| ssh2-enum-algos:

|   kex_algorithms (7)

|       ecdh-sha2-nistp256

|       ecdh-sha2-nistp384

|       ecdh-sha2-nistp521

|       diffie-hellman-group-exchange-sha256

|       diffie-hellman-group-exchange-sha1

|       diffie-hellman-group14-sha1

|       diffie-hellman-group1-sha1

|   server_host_key_algorithms (3)

|       ssh-rsa

|       ssh-dss

|       ecdsa-sha2-nistp256
```

```
|   encryption_algorithms (8)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       aes192-cbc
|       aes256-cbc
|   mac_algorithms (4)
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
```

Technical Support

Execute the diagnostic command ***show tech_support*** to send information to Pica8 Technical Support and receive a diagnostic report back.

Executing the Diagnostic Command

```
admin@XorPlus> show tech_support
Start......
Item 1: Display version finished!
Item 2: Display interface finished!
Item 3: Display pica configuration finished!
Item 4: Display system config files finished!
Item 5: Display system process finished!
Item 6: Display fdb table finished!
Item 7: Display fdb entries finished!
Item 8: Display ospf neighbors finished!
Item 9: Display ospf interfaces finished!
Item 10: Display kernel route table finished!
Item 11: Display kernel ipv4 neigh table finished!
Item 12: Display kernel ipv6 neigh table finished!
Item 13: Display kernel neigh vrf finished!
Item 14: Display hard-route table finished!
Item 15: Display system hard-route for host finished!
Item 16: Dispaly system spanning tree interfaces finished!
Item 17: Dispaly spanning tree  bridge finished!
Item 18: Display vlans table finished!
Item 19: Display vlan-interfaces finished!
Item 20: Display core-dump finished!
Item 21: Display system uptime finished!
Item 22: Display arp table!
Item 23: Display neighbor table!
Item 24: Display routes table!
Item 25: Display ipv4 routes in hardware table!
Item 26: Display ipv6 routes in hardware table!
Item 27: Display ipv4 hosts in hardware table!
Item 28: Display ipv6 hosts in hardware table!
Item 29: Display copp statistics!
Item 30: Display mlag domain!
Item 31: Display mlag link!
Item 32: Display mlag config consistency!
Item 33: Display mlag statistic!
Item 34: Display license!
Item 35: Display set!
Item 36: Get error event from log!
Item 37: Display frr configuration finished!
Process BCM commands, total count=47
The information has been stored in /tmp/XorPlus-201307052220-techSupport.log, please forward to support@pica8.com
admin@XorPlus>
```

General PICOS FAQ

We have summarized the general PICOS FAQ here, please download it from the following link:

General_PICOS_FAQ.docx

Traceoptions Configuration Commands

set interface traceoptions flag config disable true

set interface traceoptions flag ethernet-switching-options disable true
set protocols mlag traceoptions all disable false
set interface traceoptions flag neighbor-event disable true
set interface traceoptions flag packets disable true
set interface traceoptions flag route-event disable true
set interface traceoptions flag static-ethernet-switching disable true
set interface traceoptions line-card statistic disable true
set interface traceoptions line-card trace-level all disable true
set interface traceoptions line-card trace-level api debug disable true
set interface traceoptions line-card trace-level api error disable true
set interface traceoptions line-card trace-level api information disable true
set interface traceoptions line-card trace-level api warning disable true
set interface traceoptions line-card trace-level sdk debug disable true
set interface traceoptions line-card trace-level sdk error disable true
set interface traceoptions line-card trace-level sdk information disable true
set interface traceoptions line-card trace-level sdk warning disable true
set interface traceoptions line-card trace-level xrl debug disable true
set interface traceoptions line-card trace-level xrl error disable true
set interface traceoptions line-card trace-level xrl information disable true
set interface traceoptions line-card trace-level xrl warning disable true
set interface traceoptions line-card trace-type all disable true
set interface traceoptions line-card trace-type configuration disable true
set interface traceoptions line-card trace-type link-change disable true
set interface traceoptions line-card trace-type mac-update disable true
set interface traceoptions line-card trace-type packet disable true
set interface traceoptions line-card trace-type packet-receive disable true
set interface traceoptions line-card trace-type packet-transmit disable true
set interface traceoptions line-card trace-type statistics disable true

Displaying the Debugging Message

User can configure the debugging message in a current window.

Syslog Monitor On

```
admin@XorPlus> syslog monitor on
Nov 21 2000 22:27:39 XorPlus local0.warn : [SIF]Interface ge-1/1/3, changed state to up
Nov 21 2000 22:27:41 XorPlus local0.warn : root logined the switch
Nov 21 2000 22:41:18 XorPlus local0.info xinetd[1102]: START: telnet pid=7650 from=10.10.50.16
Nov 21 2000 22:41:23 XorPlus authpriv.debug login[7651]: pam_unix(login:account): account admin has password change
Nov 21 2000 22:41:26 XorPlus local0.warn : admin logined the switch
Nov 21 2000 22:55:58 XorPlus local0.info xinetd[1102]: START: telnet pid=8039 from=10.10.51.16
Nov 21 2000 22:56:01 XorPlus authpriv.debug login[8040]: pam_unix(login:account): account root has password changed
Nov 21 2000 23:31:13 XorPlus local0.info xinetd[1102]: START: telnet pid=9028 from=10.10.50.16
Nov 21 2000 23:31:16 XorPlus authpriv.debug login[9029]: pam_unix(login:account): account admin has password change
Nov 21 2000 23:31:21 XorPlus local0.warn : admin logined the switch
admin@XorPlus>
```

PICOS Routing and Switching Configuration Guide . . . 44
PICOS Supported Features . . . 52
Collection of Feature Specification of Different Platforms . . . 84
Command-Line Interface . . . 86
From Linux Shell to L2/L3 Shell . . . 87
Operation Mode and Configuration Mode . . . 88
Displaying the Current Configuration . . . 89
Display Setting Configuration . . . 90
Rolling Back a Configuration . . . 91
Managing Configuration Files . . . 92
Saving and Loading Configuration Files . . . 94
Commit Confirmed . . . 95
Commit Check . . . 96
Commit Failed and Exit Discard . . . 98
Configuring a Command Alias . . . 99
Configure L2/L3 from Linux Shell . . . 100
Bash Linux Shell . . . 101
PicOS Upgrade and Configuration Change . . . 102
Set CLI . . . 103
CLI Configuration . . . 104
Configuring Multi-window Command Configuration Display on The User Terminal . . . 105
Configuration Saving Guide . . . 106
System Administration . . . 107
Configuring Management Interface . . . 109
In-Band Management Interface . . . 110
Configuring In-Band Management Interface . . . 111
Default Settings for In-Band Management Interface on S3410 Series Switches . . . 112
Out-of-band Management Interface . . . 114
Configuring Port Speed of eth0 Out-of-Band Management Interface . . . 115
Default Settings for Out-of-band Management Interface . . . 116
Configuring User Account and Login Banner . . . 117
Configuring SSH and Telnet Parameters . . . 118
Configuring the Log-in ACL . . . 120
AAA Configuration Guide . . . 121
Introduction . . . 122
Configuration Notes of AAA . . . 124
TACACS+ Configuration . . . 125
RADIUS Configuration . . . 128
Local Authentication Configuration . . . 131
Sample configuration file on the AAA server . . . 132
NAC Configuration Guide . . . 133
Configuration Notes of NAC . . . 134
Configuring NAC . . . 135
Configuration Example of NAC . . . 137
Example for Configuring 802.1X Authentication . . . 138

Example for Configuring MAB Authentication . . . 140
Example for Configuring CWA Authentication . . . 142
Example for Configuring Multiple Authentication Modes . . . 145
Typical Configuration of NAC . . . 148
Example for Configuring NAC (PacketFence as the Authentication Server) . . . 149
Solution Documents Download . . . 154
References . . . 155
Principle of NAC . . . 156
Configuring NTP and the Time Zone Parameter . . . 174
Configuring PTP . . . 175
Configuring the linux-config-unreliable . . . 179
Configuring IPFIX . . . 180
Configuring sFlow . . . 181
Configuring the Syslog Log Level . . . 183
Configuring the Syslog Disk and Syslog Server . . . 184
Displaying System Information . . . 185
IPv6 Management Support . . . 188
Configuring NETCONF . . . 189
SNMP Configuration . . . 192
Configuring SNMPv2 . . . 193
Configuring SNMPv3 . . . 195
Configuring SNMP ACL . . . 198
Pica8 Private MIB . . . 200
pica_private_mib.my . . . 202
pica_private_trap_mib.my . . . 212
Pica8 Public MIB . . . 217
SNMP Monitoring and Integration with Zabbix . . . 218
PoE Configuration Guide . . . 219
Configuring PoE . . . 220
PoE over LLDP Power Negotiation . . . 221
UPoE . . . 224
Configuring Perpetual PoE . . . 225
Configuring USB Disable . . . 226
Configuring CPU Usage Alarm Threshold . . . 227
Configuring MAC Usage Alarm Threshold . . . 229
Mirror Configuration . . . 231
Introduction of Mirroring . . . 232
Configuration Notes of Mirroring . . . 235
Configuring Mirror . . . 236
Example for Configuring Local Port Mirroring . . . 238
Example for Configuring ERSPAN . . . 240
Example for Configuring ACL-based ERSPAN . . . 243
Configuring gNMI-gRPC Based Telemetry Technology . . . 246
Remote Network Monitoring (RMON) . . . 248
Overview of RMON . . . 249

Configuring RMON . . . 250
Example for Configuring RMON . . . 252
RESTCONF Configuration . . . 255
Introduction of RESTCONF . . . 256
RESTCONF Operation Methods . . . 263
Configuring RESTCONF . . . 272
EFM OAM Configuration . . . 274
Introduction of EFM OAM . . . 275
Configuring EFM OAM . . . 279
Configure Telnet to Access to the Remote Device . . . 285
Interface Management Configuration Guide . . . 286
Ethernet Ports Management Configuration . . . 287
Port Naming Conventions . . . 288
Physical Ethernet Port Configuration . . . 290
Configuring Port Breakout and Merge . . . 291
Overview of Port Breakout . . . 292
100GE and 40GE . . . 293
400GE and 200GE . . . 295
800GE . . . 299
Interface Rate Configuraion . . . 302
Introduction of Interface Rate . . . 303
Configuring the Force Rate of an Interface . . . 306
Configuring the Auto-Negotiation Mode . . . 307
Port Security Configuration . . . 309
CDR Function Configuration . . . 314
Time Domain Reflectometry (TDR) . . . 315
Configuring Port Mapping On S4148 Series Switch . . . 317
10G-Base-KR Interface Configuration . . . 319
Forwarding Error Correction (FEC) . . . 322
Configuring the Loopback Interface . . . 324
Layer 3 VLAN Interface Configuration . . . 325
Configuring Routed Interface . . . 327
Introduction of Routed Interface . . . 328
Configuration Notes of Routed Interface . . . 331
Configuring Routed Interface and Sub-interface . . . 332
Example for Configuring Routed Interface . . . 333
Uplink Failure Detection . . . 336
Layer 2 Switching Configuration . . . 339
Static MAC entries and Dynamic MAC Address Learning . . . 341
Cut-Through Switching Method . . . 342
MLAG Configuration . . . 343
Principle of MLAG . . . 344
Configuration Notes and Constraints . . . 364
Configuring MLAG . . . 365
Configuration Example of MLAG . . . 366

Example for Configuring a Basic MLAG . . . 367
Example for Configuring MLAG with Active-Active-VRRP . . . 371
Example for Configuring MLAG with DHCP Relay . . . 378
Example for Configuring MLAG with DHCP Snooping . . . 384
Example for Configuring MLAG with IGMP Snooping . . . 388
Example for Configuring MLAG with Rapid PVST+ . . . 392
Example for Configuring MLAG with VXLAN . . . 398
MLAG Maintenance and Troubleshooting . . . 403
How to bind a LAG interface to the MLAG link? . . . 404
How to check whether the VLAN configuration on the two peer-link ports are consistent? . . . 405
How to confirm whether the MAC address table has been correctly synchronized? . . . 406
How to enable MLAG traceoptions . . . 407
How to ensure the reliability of the peer link? . . . 408
How to verify configurations on MLAG peer are consistent? . . . 409
How to verify MLAG link status? . . . 411
How to verify MLAG neighbor status? . . . 412
How to verify that the peer link connection status is normal? . . . 413
How to view and clear MLAG statistics? . . . 414
VLAN Configuration . . . 415
Configuring MAC-based VLAN . . . 416
MAC Trace . . . 418
Configuring Port-based VLAN . . . 421
GVRP . . . 426
Overview of GVRP . . . 427
Configuring GVRP . . . 428
Example for Configuring GVRP . . . 429
MVRP . . . 431
Overview of MVRP . . . 432
Configuring MVRP . . . 433
Example for Configuring MVRP . . . 434
Q-in-Q Basic Port Configuration . . . 437
Private VLAN Configuration Guide . . . 444
Introduction of PVLAN . . . 445
Configuration Notes of PVLAN . . . 453
Configuring PVLAN . . . 454
Example for Configuring PVLAN . . . 455
Example for Configuring DHCP Snooping with PVLAN . . . 457
Voice VLAN Configuration Guide . . . 460
Principle of Voice VLAN . . . 461
Configuration Notes of Voice VLAN . . . 464
Configuring Voice VLAN . . . 465
Configuration Example of Voice VLAN . . . 466
Link Aggregation Configuration . . . 469
Static Link Aggregation (LAG) Configuration . . . 470
Link Aggregation Control Protocol (LACP) Configuration . . . 471

LAG Hashing Configuration . . . 472
LAG Hashing Configuration and Example . . . 473
LAG Hash Mapping . . . 474
Resilient LAG Hashing Configuration and Example . . . 475
LACP Fallback . . . 476
Configuring LACP Fast Rate . . . 480
LAG Specification of Different Platforms . . . 481
Symmetric Hash for LAG Configuration Example . . . 482
LLDP Configuration (Link Layer Discovery Protocol) . . . 484
LLDP MED Configuration . . . 486
MSTP Configuration . . . 488
MSTP Configuration Example . . . 493
Rapid PVST+ Configuration . . . 503
Rapid PVST+ Configuration Example . . . 508
BPDU Tunneling Configuration . . . 511
UDLD Configuration . . . 515
LFS Configuration . . . 519
Storm Control in Ethernet Port Configuration . . . 520
Ethernet Ring Protection Switching (ERPS) . . . 521
Overview of ERPS . . . 522
Configuration Notes and Constraints of ERPS . . . 527
Configuring ERPS . . . 528
Example for Configuring ERPS (Single Ring) . . . 530
Example for Configuring ERPS (Intersection Rings) . . . 536
Loopback Detection . . . 544
Overview of Loopback Detection . . . 545
Configuring Loopback Detection . . . 547
Layer 3 Routing Configuration . . . 550
ARP Configuration . . . 553
Configuring ARP . . . 554
Dynamic ARP Inspection (DAI) . . . 555
Flushing ARP and the Neighbor Table . . . 559
Configuring IP Routing . . . 560
Static Routing Configuration . . . 562
Configuring Static Routes . . . 563
Example for Configuring IPv4 Static Routes . . . 565
VRF Configuration Guide . . . 568
Introduction to VRF . . . 569
Configuration Notes of VRF . . . 572
Configuring a User-defined VRF . . . 573
Enabling Management VRF . . . 574
Example for Configuring Basic VRF . . . 575
DHCP Configuration . . . 577
Introduction to DHCP . . . 578
Configuration Notes of DHCP . . . 582

Configuring DHCP Server (IPv4) . . . 583
Configuring DHCP Relay . . . 588
Configuring DHCP Relay (IPv4) . . . 589
Example for Configuring DHCPv6 Relay . . . 592
Example for Configuring DHCP Relay over GRE Tunnel . . . 594
Configuring DHCP Snooping . . . 597
Configuring DHCP Snooping (IPv4) . . . 598
Configuring DHCPv6 Snooping (IPv6) . . . 601
Typical Configuration Example for DHCP Relay and DHCP Snooping . . . 604
DHCPv6 Guard Configuration . . . 606
Overview of DHCPv6 Guard . . . 607
Configuring DHCPv6 Guard . . . 610
Example for Configuring DHCPv6 Guard . . . 612
RFC Lists . . . 614
Default Administrative Distance Values . . . 615
OSPF (Open Shortest Path First) . . . 616
OSPF Overview . . . 617
Basic OSPF Configuration Tasks . . . 618
Configuring OSPF Route Summarization . . . 620
Basic OSPF Configuration Example . . . 621
OSPF Area Type Configuration Example: NSSA, Stub and Standard Areas . . . 624
OSPF Stub and NSSA Areas with no-summary . . . 627
OSPF Area Range Configuration Guide . . . 628
OSPF Route Redistribution and Route Maps . . . 630
Example for Configuring OSPF with Different VRFs . . . 632
OSPFv3 Configuration Guide . . . 636
OSPF Multi-Instance Support . . . 638
OSPF GR . . . 640
ECMP (Equal-Cost Multipath Routing) Configuration . . . 648
Symmetric Hash for ECMP Configuration Example . . . 651
VRRP Configuration . . . 653
Principle of VRRP . . . 654
Configuration Notes of VRRP . . . 659
Configuring Standard VRRP . . . 660
Configuring Active-Active VRRP . . . 662
VRRP Configuration Example . . . 664
Example for Configuring Standard VRRPv3 for IPv4 . . . 665
Example for Configuring Active-Active VRRPv3 for IPv4 . . . 667
Example for Configuring Active-Active VRRPv3 for IPv6 . . . 670
IPv4/IPv6 BGP Configuration . . . 673
BGP Introduction . . . 674
BGP Regular Expressions . . . 677
Basic BGP Configuration . . . 678
Configuring BGP Security . . . 680
Configuring a BGP Route Reflector . . . 681

Configuring BGP Timers . . . 682
Configuring BGP Route Aggregation . . . 684
Configuring BGP Dynamic Neighbors . . . 685
Configuring eBGP Multihop . . . 686
Configuring Removing and Replacing Private ASNs from the AS Path . . . 687
Configuring BGP Multipath . . . 688
Configuring ebgp-requires-policy . . . 689
Enable BGP Read-only Mode . . . 690
Configuring Route Maps for Route Updates . . . 691
BGP Unnumbered . . . 692
Overview of BGP Unnumbered . . . 693
Example for Configuring Basic BGP Unnumbered . . . 694
Example for Configuring BGP Unnumbered EVPN Fabric . . . 698
Configuring BGP Attribute . . . 703
Configuring the AS_Path Attribute . . . 704
Configuring the BGP Community Attribute . . . 705
Configuring the MED Attribute . . . 706
Configuring the Next_Hop Attribute . . . 707
Configuration Examples . . . 708
Example for Configuring Basic BGP Functions . . . 709
Example for Configuring a BGP Route Reflector . . . 715
Example for Configuring BGP Load Balancing . . . 718
Routing Map Configuration . . . 723
Routing Map Introduction . . . 724
Configuring Filters . . . 725
Configuring a Community Filter . . . 726
Configuring a Large Community Filter . . . 727
Configuring an AS_Path Filter . . . 728
Configuring an Extended Community Filter . . . 729
Configuring an IP Prefix List . . . 730
Configuring a Routing Map . . . 731
Example for Filtering the Routes to Be Advertised and Receiving . . . 733
IPv6 Support . . . 737
IPv6 Neighbor Discovery Configuration . . . 739
PICOS L2/L3 Support for IPv6 . . . 741
Enable Path MTU Discovery . . . 742
IPv6 Neighbor Discovery Inspection . . . 743
Overview of ND Inspection . . . 744
Configuring ND Inspection . . . 747
Example for ND Inspection . . . 748
IPv6 Neighbor Discovery Snooping . . . 750
Overview of ND Snooping . . . 751
Operation Mechanism of ND Snooping . . . 755
Configuring ND Snooping . . . 757
Example for ND Snooping . . . 758

VRF Route Leaking Configuration . . . 760
BGP Route Leaking Configuration Example . . . 761
Static Route Leaking Example . . . 765
Bidirectional Forwarding Detection (BFD) . . . 768
Introduction of BFD . . . 769
Configuring BFD . . . 770
Configuring Static BFD . . . 771
Configuring Dynamic BFD . . . 772
Configuration Examples of BFD . . . 774
Example for Configuring Single-Hop BFD . . . 775
Example for Configuring Multi-Hop BFD . . . 777
Example for Configuring BFD for BGP . . . 780
Example for Configuring BFD for OSPF . . . 783
Example for Configuring BFD for PIM-SM . . . 786
RFC Lists for BFD . . . 788
RIP/RIPng Configuration . . . 789
RIP/RIPng Overview . . . 790
Enabling RIP/RIPng . . . 791
Configuring RIP Version . . . 792
Configuring RIP Route Redistribute . . . 793
Configuring RIPv2 Authentication . . . 796
Configuring RIP to Advertise Default Routes . . . 797
Example for Configuring Basic RIP . . . 798
Example for Configuring Basic RIPng . . . 801
RFC Lists for RIP/RIPng . . . 804
Policy-Based Routing (PBR) . . . 805
Overview of PBR . . . 806
Configuring Policy-Based Routing . . . 807
Example for Configuring Policy-Based Routing . . . 809
IPv4 Source Guard (IPSG for IPv4) . . . 811
IPv6 Source Guard (IPSG for IPv6) . . . 815
IPv6 RA Guard Configuration . . . 819
IS-IS Configuration . . . 821
IS-IS Overview . . . 822
Configuring IS-IS Basic Function . . . 824
Configuring IS-IS Authentication . . . 826
Configuring LSP Packet Attributes . . . 828
Customizing Routes for IS-IS . . . 830
Configuring IS-IS Timers . . . 832
Configuring the Interval for Sending Hello Messages . . . 833
Configuring the Hello-Multiplier for the Neighbor Holding Time . . . 834
Configuring the Interval for Sending CSNP Messages . . . 835
Configuring the Interval for Sending PSNP Messages . . . 836
Controlling IS-IS Routing Information Exchange . . . 837
Configuring IS-IS Advertising Default Routes . . . 838

Configuring IS-IS Introducing External Routes . . . 839
Adjusting SPF Calculation Time . . . 840
Configuration Examples of IS-IS . . . 841
Basic IS-IS Configuration Example . . . 842
Configuration Example of Interaction Between IS-IS and BGP . . . 846
IP Multicast Routing Configuration . . . 850
IGMP Configuration . . . 851
PIM Configuration Guide . . . 853
Introduction of PIM . . . 854
Configuring PIM-SM . . . 856
Example for Configuring PIM-SM . . . 858
Example for Configuring PIM-SSM . . . 861
Example for Configuring PIM over GRE Tunnel . . . 864
RFC List of PIM . . . 868
Example for Configuring Basic PIM-SM . . . 869
IGMP Snooping Configuration Guide . . . 872
Introduction to IGMP Snooping . . . 873
Enable Unknown Multicast Traffic Flooding with IGMP Snooping Enabled . . . 874
Configuring IGMP Snooping . . . 875
Example for Configuring Basic IGMP Snooping . . . 876
Example for Configuring IGMP Snooping with IGMP . . . 879
RFC List . . . 881
Multicast Source Discovery Protocol (MSDP) . . . 882
Introduction of MSDP . . . 883
Example for Configuring PIM-SM Inter-domain Multicast Using MSDP . . . 884
Example for Configuring Anycast RP . . . 888
RFC Lists of MSDP . . . 893
Multicast VLAN Registration (MVR) . . . 894
Overview of MVR . . . 895
Configuration Notes and Constraints of MVR . . . 897
Configuring MVR . . . 898
ACL Configuration . . . 900
Configuring Basic ACL . . . 901
Configuring Time Range . . . 904
QoS Configuration . . . 907
Weighted Random Early Detection . . . 908
WRED Overview . . . 909
WRED Configuration Tasks . . . 910
WRED Configuration Example . . . 912
QoS Principle . . . 914
SP Configuration Example . . . 915
QoS Configuration Example . . . 917
Configuring Classifier-based QoS . . . 918
Configuring ACL-based QoS . . . 920
PFC Configuration Example . . . 923

ACL-based Traffic Policer . . . 925
CoPP Configuration Guide . . . 928
Principle . . . 929
Default Settings for CoPP (N2224PX-ON/N2248X-ON/N3208PX-ON) . . . 931
CoPP Configuration . . . 939
Configuration Notes . . . 940
Configuring CoPP . . . 941
Configuration Example . . . 943
Default Settings for CoPP . . . 949
Queue-based Rate Limiting . . . 961
Interface-based Rate Limiting . . . 963
Configuring Ingress Interface-based Rate Limiting . . . 964
Configuring Egress Interface-based Rate Limiting . . . 965
WRR Configuration Example . . . 967
Buffer Management . . . 970
WFQ Configuration Example . . . 974
VXLAN Configuration . . . 977
VXLAN Base Configuration Example . . . 978
VXLAN Routing . . . 980
Cross-Subnet Packet Forwarding Process . . . 981
Example for Configuring VXLAN for Different Subnets . . . 983
VXLAN Configuration Guide . . . 987
VXLAN ECMP Configuration . . . 992
BGP EVPN Configuration Guide . . . 997
BGP EVPN Route Types . . . 998
Anycast Gateway for EVPN Distributed Networks . . . 1000
EVPN Symmetric Routing Configuration Example . . . 1004
EVPN Asymmetric Routing Example . . . 1009
EVPN With NAC Configuration Guide . . . 1014
EVPN Multihoming Configuration Guide . . . 1019
EVPN Enhancements . . . 1034
Introduction to BGP EVPN . . . 1035
Generic Routing Encapsulation Protocol (GRE) . . . 1039
Overview . . . 1040
GRE Configuration Example . . . 1042
MPLS Configuration . . . 1045
MPLS Overview . . . 1046
Configuration Restrictions and Guidlines . . . 1048
Basic MPLS LDP Configuration . . . 1049
(Optional) Configuring MPLS LDP Security . . . 1052
(Optional) Configuring MPLS LDP Timers . . . 1054
(Optional) Configuring MPLS LDP to Allocate Labels for Host Routes Only . . . 1057
(Optional) Configuring MPLS LDP PHP (Penultimate Hop Popping) . . . 1058
Example for Configuring MPLS LDP . . . 1059
RFC Lists for MPLS . . . 1063

Lossless Network Configuration . . . 1064
Lossless Network Introduction . . . 1065
Application Scenarios . . . 1067
Key Features of Lossless Network . . . 1069
Configuring Priority-based Flow Control (PFC) . . . 1070
Enabling PFC Function . . . 1071
Configuring PFC Buffer . . . 1074
Configuring PFC Watchdog . . . 1077
Configuring PFC Deadlock Prevention . . . 1082
Configuring Explicit Congestion Notification (ECN) . . . 1085
Configuring Easy ECN . . . 1089
PFC and ECN Statistical Reporting through gRPC . . . 1091
Configuring Dynamic Load Balancing . . . 1092
Typical Configuration Example of Lossless Network . . . 1095
OpenFlow in Crossflow Mode . . . 1099
Crossflow Mode Introduction . . . 1100
CrossFlow Mode Known Limitations . . . 1103
Crossflow Basic Configuration . . . 1104
Configuration Example1 in Crossflow Mode . . . 1105
Configuration Example2 in Crossflow Mode . . . 1110
Example for Configuring STM Resource Allocation . . . 1113
Multi-action in crossflow mode . . . 1115
PICOS Routing and Switching Command Reference . . . 1117
Command-Line Interface Commands . . . 1139
copy running-config startup-config . . . 1140
set cli idle-timeout . . . 1141
set cli screen-length . . . 1142
set cli terminal . . . 1143
syslog monitor . . . 1144
syslog notify . . . 1145
hwclock . . . 1146
rollback . . . 1148
System Management Commands . . . 1149
NAC Configuration Commands . . . 1153
set protocols dot1x aaa radius authentication server-ip . . . 1154
set protocols dot1x aaa radius authentication server-ip priority . . . 1155
set protocols dot1x aaa radius authentication server-ip retry-num . . . 1156
set protocols dot1x aaa radius authentication server-ip retry-interval . . . 1157
set protocols dot1x aaa radius authentication server-ip detect-interval . . . 1158
set protocols dot1x interface auth-mode 802.1x . . . 1159
set protocols dot1x interface auth-mode 802.1x fallback-to-web disable . . . 1160
set protocols dot1x interface auth-mode mac-radius . . . 1161
set protocols dot1x interface auth-mode web . . . 1162
set protocols dot1x interface authentication-open disable . . . 1163
set protocols dot1x aaa radius dynamic-author client . . . 1164

set protocols dot1x aaa radius dynamic-author client shared-key . . . 1165
set protocols dot1x aaa radius nas-ip . . . 1166
set protocols dot1x aaa radius accounting disable . . . 1167
set protocols dot1x interface host-mode . . . 1168
set protocols dot1x block-vlan-id . . . 1169
set protocols dot1x server-fail-vlan-id . . . 1170
set protocols dot1x filter sequence from destination-address-ipv4 . . . 1171
set protocols dot1x filter sequence from destination-address-ipv6 . . . 1172
set protocols dot1x filter sequence from destination-port . . . 1173
set protocols dot1x filter sequence from ether-type . . . 1174
set protocols dot1x filter sequence from source-address-ipv4 . . . 1175
set protocols dot1x filter sequence from source-address-ipv6 . . . 1176
set protocols dot1x filter sequence from source-port . . . 1177
set protocols dot1x filter sequence from protocol . . . 1178
set protocols dot1x filter sequence then action . . . 1179
run show dot1x all . . . 1180
run show dot1x interface . . . 1181
run show dot1x server . . . 1183
run show dot1x dynamic filter . . . 1184
run show dot1x downloadable filter . . . 1185
run show dot1x interface statistics gigabit-ethernet . . . 1186
set protocols dot1x server-fail recovery-method . . . 1187
set protocols dot1x aaa radius authentication server-ip consecutive-detect-num . . . 1188
set protocols dot1x aaa vrf mgmt-vrf . . . 1189
set protocols dot1x interface session-timeout . . . 1190
set protocols dot1x interface recovery-timeout . . . 1191
set protocols dot1x server-fail recovery-timeout . . . 1192
set protocols dot1x interface max-sessions . . . 1193
set protocols dot1x max-sessions-per-port . . . 1194
set protocols dot1x aaa radius authentication server-ip auth-port . . . 1195
set protocols dot1x aaa radius authentication server-ip acct-port . . . 1196
set protocols dot1x aaa radius dynamic-author client port . . . 1197
run show dot1x radius-port . . . 1198
set protocols dot1x filter sequence from destination-mac-address . . . 1199
set protocols dot1x filter sequence from vlan . . . 1200
SNMP Configuration Commands . . . 1201
set protocols snmp trap-group targets security-name . . . 1202
set protocols lldp snmp-trap . . . 1203
set protocols snmp trap-group event cpu-threshold enable . . . 1204
set protocols snmp trap-group event cpu-threshold high . . . 1205
set protocols snmp trap-group event cpu-threshold interval . . . 1206
set protocols snmp trap-group event cpu-threshold low . . . 1207
set protocols snmp trap-group event mac-threshold enable . . . 1208
set protocols snmp trap-group event mac-threshold interval . . . 1209
set protocols snmp trap-group event mac-threshold limit . . . 1210

set protocols snmp trap-group vrf mgmt-vrf . . . 1211
set protocols snmp trap-group version . . . 1212
set protocols snmp v3 enable . . . 1213
set protocols snmp v3 usm-user . . . 1214
set protocols snmp v3 usm-user group . . . 1215
set protocols snmp v3 group notify-view . . . 1216
set protocols snmp v3 group read-view . . . 1217
set protocols snmp v3 group write-view . . . 1218
set protocols snmp v3 group security-level . . . 1219
set protocols snmp v3 usm-user authentication-mode . . . 1220
set protocols snmp v3 usm-user authentication-key . . . 1221
set protocols snmp v3 usm-user privacy-mode . . . 1222
set protocols snmp v3 usm-user privacy-key . . . 1223
set protocols snmp v3 mib-view subtree mask . . . 1224
set protocols snmp v3 mib-view subtree type . . . 1225
set protocols snmp trap-group source-interface . . . 1226
set protocols snmp community . . . 1227
set protocols snmp community authorization . . . 1228
set protocols snmp community clients . . . 1229
set protocols snmp contact . . . 1230
set protocols snmp location . . . 1231
run show snmp statistics . . . 1232
Mirror Configuration Commands . . . 1233
set interface ethernet-switching-options analyzer input . . . 1234
set interface ethernet-switching-options analyzer output . . . 1235
set interface ethernet-switching-options analyzer erspan input . . . 1236
set interface ethernet-switching-options analyzer erspan output source-ip . . . 1237
set interface ethernet-switching-options analyzer erspan output dest-ip . . . 1238
set interface ethernet-switching-options analyzer erspan output vrf . . . 1239
run show analyzer . . . 1240
set firewall filter sequence then erspan source-ip . . . 1241
set firewall filter sequence then erspan dest-ip . . . 1242
set firewall filter sequence then erspan vrf . . . 1243
set firewall filter sequence then erspan ttl . . . 1244
RMON Commands . . . 1245
run show rmon alarms . . . 1246
run show rmon eventlog . . . 1247
run show rmon events . . . 1248
run show rmon history . . . 1249
run show rmon statistics . . . 1250
set protocols snmp rmon alarm falling-event-index . . . 1251
set protocols snmp rmon alarm falling-threshold . . . 1252
set protocols snmp rmon alarm interval . . . 1253
set protocols snmp rmon alarm owner . . . 1254
set protocols snmp rmon alarm rising-event-index . . . 1255

set protocols snmp rmon alarm rising-threshold . . . 1256
set protocols snmp rmon alarm sample-type . . . 1257
set protocols snmp rmon alarm variable . . . 1258
set protocols snmp rmon event community . . . 1259
set protocols snmp rmon event description . . . 1260
set protocols snmp rmon event owner . . . 1261
set protocols snmp rmon event type . . . 1262
set protocols snmp rmon history buckets . . . 1263
set protocols snmp rmon history interface . . . 1264
set protocols snmp rmon history interval . . . 1265
set protocols snmp rmon history owner . . . 1266
set protocols snmp rmon statistics interface . . . 1267
set protocols snmp rmon statistics owner . . . 1268
RESTCONF Commands . . . 1269
set protocols restconf . . . 1270
set protocols restconf port . . . 1271
set protocols restconf traceoptions flag config disable . . . 1272
set protocols restconf traceoptions flag all disable . . . 1273
set protocols restconf traceoptions flag datastore disable . . . 1274
run show system boot-messages . . . 1275
run show system connections . . . 1276
run show system core-dumps . . . 1279
run show system cpu-usage . . . 1280
run show system date . . . 1281
run show system fan . . . 1282
run show system memory-usage . . . 1283
run show system name . . . 1284
run show system ntp-status . . . 1285
run show system os . . . 1286
run show system processes brief . . . 1287
run show system processes detail . . . 1289
run show system rollback compare to . . . 1291
run show system rollback file . . . 1292
run show system rollback list . . . 1294
run show system rpsu . . . 1295
run show system serial-number . . . 1296
run show system temperature . . . 1297
run show system uptime . . . 1298
run show system users . . . 1299
set system aaa local disable . . . 1300
set system aaa radius accounting disable . . . 1301
set system aaa radius accounting server-ip . . . 1302
set system aaa radius accounting server-ip port . . . 1303
set system aaa radius accounting server-ip shared-key . . . 1304
set system aaa radius accounting server-ip timeout . . . 1305

set system aaa radius authorization disable 1306
set system aaa radius authorization server-ip 1307
set system aaa radius authorization server-ip port 1308
set system aaa radius authorization server-ip shared-key 1309
set system aaa radius authorization server-ip timeout 1310
set system aaa radius vrf mgmt-vrf 1311
set system aaa tacacs-plus accounting 1312
set system aaa tacacs-plus authorization 1313
set system aaa tacacs-plus auth-type 1314
set system aaa tacacs-plus disable 1315
set system aaa tacacs-plus key 1316
set system aaa tacacs-plus port-number 1317
set system aaa tacacs-plus timeout 1318
set system aaa tacacs-plus server-ip 1319
set system aaa tacacs-plus source-interface 1320
set system aaa local-auth-fallback disable 1321
set system aaa tacacs-plus vrf mgmt-vrf 1322
set system hostname 1323
set system inband vlan-interface 1324
set system inband loopback 1325
set system inband routed-interface 1326
set system inband enable 1327
system login-acl network 1328
system login announcement 1329
system login user 1330
system login user admin class 1331
set system login user authentication plain-text-password 1332
system login user class 1333
set system timezone 1334
set system ntp server-ip 1335
set system ntp source-interface 1336
set system ntp vrf mgmt-vrf 1337
set interface gigabit-ethernet ptp mode 1338
set system services ssh connection-limit 1339
set system services ssh disable 1340
set system services ssh protocol-version v2 1341
set system services ssh rate-limit 1342
set system services ssh root-login 1343
set system services ssh idle-timeout 1344
set system services ssh port 1345
set system snmp-acl security-name network 1346
set system syslog server-ip 1347
set system syslog local-file 1348
set system syslog vrf mgmt-vrf 1349
set system usb disable 1350

set system management-ethernet eth0 ip-address {IPv4 | IPv6} . . . 1351
set system management-ethernet eth0 ip-gateway {IPv4 | IPv6} . . . 1352
show system management-ethernet . . . 1353
run request system reboot . . . 1354
run show system hwinfo . . . 1356
ping . . . 1357
traceroute . . . 1359
tftp . . . 1360
set protocols sflow collector vrf mgmt-vrf . . . 1361
scp . . . 1362
set system login banner . . . 1363
upgrade2 image-file . . . 1364
upgrade2 image-file backup-file . . . 1365
upgrade2 image-file factory-default . . . 1367
upgrade2 image-file use-prev-config . . . 1368
set system dns-server-ip . . . 1369
set system console idle-timeout . . . 1370
set system login multiline-banner message . . . 1371
set system login multiline-announcement message . . . 1372
set system aaa radius source-interface . . . 1373
set protocols grpc enable . . . 1374
set protocols grpc port . . . 1375
set system ztp enable . . . 1376
telnet . . . 1377
set system start-shell-sh password . . . 1379
set system services telnet disable . . . 1380
set system services web disable . . . 1381
Interface Configuration Commands . . . 1382
Port Security Commands . . . 1385
set interface gigabit-ethernet port-security mac-address vlan . . . 1386
set interface gigabit-ethernet port-security mac-limit . . . 1387
set interface gigabit-ethernet port-security sticky . . . 1388
set interface gigabit-ethernet port-security violation . . . 1389
set interface gigabit-ethernet port-security block . . . 1390
set interface ethernet-switching-options port-error-discard timeout . . . 1391
run show port-security brief . . . 1392
run show port-security address . . . 1393
run show port-security interface . . . 1394
run clear port-security port-error . . . 1396
run clear port-security sticky interface . . . 1397
run clear port-security sticky address . . . 1398
run clear port-security dynamic interface . . . 1399
run clear port-security dynamic address . . . 1400
L3 Interface . . . 1401
set l3-interface vlan-interface vrf . . . 1402

set l3-interface vlan-interface address prefix-length . . . 1403
set l3-interface loopback address . . . 1404
set l3-interface loopback disable . . . 1405
set l3-interface loopback vrf . . . 1406
set l3-interface vlan-interface rate-limit . . . 1407
set l3-interface vlan-interface mtu . . . 1408
set l3-interface vlan-interface dhcp . . . 1409
run show l3-interface vlan-interface . . . 1410
run show l3-interface . . . 1411
run show l3-interface loopback . . . 1412
run clear l3-interface statistics . . . 1413
set l3-interface routed-interface dhcp . . . 1414
set l3-interface routed-interface rate-limit . . . 1415
set l3-interface routed-interface mtu . . . 1416
set l3-interface routed-interface vrf . . . 1417
set l3-interface routed-interface address . . . 1418
set l3-interface routed-interface description . . . 1419
run show l3-interface routed-interface . . . 1420
set l3-interface vlan-interface pmtu-discovery . . . 1421
set l3-interface routed-interface pmtu-discovery . . . 1422
Routed Interface . . . 1423
run show interface routed-interface brief . . . 1424
run show vlans routed-vlan . . . 1425
set interface aggregate-ethernet routed-interface enable . . . 1426
set interface aggregate-ethernet routed-interface name . . . 1427
set interface aggregate-ethernet routed-interface sub-interface vlan-id . . . 1428
set interface gigabit-ethernet routed-interface enable . . . 1429
set interface gigabit-ethernet routed-interface sub-interface . . . 1431
set vlans reserved-vlan . . . 1432
set interface gigabit-ethernet routed-interface name . . . 1434
set interface gigabit-ethernet speed . . . 1435
Uplink Failure Detection Commands . . . 1437
run show interface ufd . . . 1438
set interface ufd link-to-monitor . . . 1439
set interface ufd link-to-disable . . . 1440
IPv6 Neighbor Discovery Protocol Command Reference . . . 1441
set l3-interface routed-interface ipv6-nd adv-interval-option . . . 1442
set l3-interface routed-interface ipv6-nd home-agent-config-flag . . . 1443
set l3-interface routed-interface ipv6-nd home-agent-lifetime . . . 1444
set l3-interface routed-interface ipv6-nd home-agent-preference . . . 1445
set l3-interface routed-interface ipv6-nd managed-config-flag . . . 1446
set l3-interface routed-interface ipv6-nd mtu . . . 1447
set l3-interface routed-interface ipv6-nd other-config-flag . . . 1448
set l3-interface routed-interface ipv6-nd prefix off-link . . . 1449
set l3-interface routed-interface ipv6-nd prefix preferred-lifetime . . . 1450

set l3-interface routed-interface ipv6-nd prefix router-address . . . 1451
set l3-interface routed-interface ipv6-nd prefix valid-lifetime . . . 1452
set l3-interface routed-interface ipv6-nd ra-fast-retrans . . . 1453
set l3-interface routed-interface ipv6-nd ra-interval . . . 1454
set l3-interface routed-interface ipv6-nd ra-lifetime . . . 1455
set l3-interface routed-interface ipv6-nd reachable-time . . . 1456
set l3-interface routed-interface ipv6-nd router-preference . . . 1457
set l3-interface routed-interface ipv6-nd suppress-ra . . . 1458
set l3-interface vlan-interface ipv6-nd adv-interval-option . . . 1459
set l3-interface vlan-interface ipv6-nd home-agent-config-flag . . . 1460
set l3-interface vlan-interface ipv6-nd home-agent-lifetime . . . 1461
set l3-interface vlan-interface ipv6-nd home-agent-preference . . . 1462
set l3-interface vlan-interface ipv6-nd managed-config-flag . . . 1463
set l3-interface vlan-interface ipv6-nd mtu . . . 1464
set l3-interface vlan-interface ipv6-nd other-config-flag . . . 1465
set l3-interface vlan-interface ipv6-nd prefix off-link . . . 1466
set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime . . . 1467
set l3-interface vlan-interface ipv6-nd prefix router-address . . . 1468
set l3-interface vlan-interface ipv6-nd prefix valid-lifetime . . . 1469
set l3-interface vlan-interface ipv6-nd ra-fast-retrans . . . 1470
set l3-interface vlan-interface ipv6-nd ra-interval . . . 1471
set l3-interface vlan-interface ipv6-nd ra-lifetime . . . 1472
set l3-interface vlan-interface ipv6-nd reachable-time . . . 1473
set l3-interface vlan-interface ipv6-nd router-preference . . . 1474
set l3-interface vlan-interface ipv6-nd suppress-ra . . . 1475
set management-ethernet-speed eth0 . . . 1476
set interface gigabit-ethernet up-mode . . . 1477
show interface bpdu-tunneling . . . 1478
show interface aggregate-ethernet <lag_name> . . . 1479
show interface aggregate-ethernet <lag_name> dot1q-tunneling . . . 1480
show interface brief . . . 1481
show interface detail . . . 1483
show interface diagnostics optics all . . . 1484
show interface ecmp max-path . . . 1485
show interface flexlink . . . 1486
show interface gigabit-ethernet <interface> . . . 1487
set interface gigabit-ethernet fec . . . 1489
set interface gigabit-ethernet family ethernet-switching vlan members . . . 1490
set interface gigabit-ethernet family ethernet-switching port-mode . . . 1491
set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol . . . 1493
set interface gigabit-ethernet ether-options 802.3ad . . . 1494
set interface gigabit-ethernet duplex auto . . . 1495
set interface gigabit-ethernet breakout-type . . . 1496
set interface gigabit-ethernet auto-speeds . . . 1498
set interface ecmp hash-mapping field vlan disable . . . 1499

set interface ecmp hash-mapping field port-source disable 1500
set interface ecmp hash-mapping field port-destination disable 1501
set interface ecmp hash-mapping field ip-source disable 1502
set interface ecmp hash-mapping field ip-protocol disable 1503
set interface ecmp hash-mapping field ip-destination disable 1504
set interface ecmp hash-mapping field ingress-interface disable 1505
set interface bpdu-tunneling destination-mac 1506
set interface aggregate-ethernet family ethernet-switching vlan members 1507
set interface aggregate-ethernet family ethernet-switching port-mode 1508
set interface aggregate-ethernet disable 1510
set interface aggregate-ethernet description 1511
set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout 1512
set interface aggregate-ethernet aggregated-ether-options lacp fallback enable 1513
set interface aggregate-ethernet aggregated-ether-options lacp 1514
set interface aggregate-ethernet 1515
run show interface port-index-mapping 1516
run show interface diagnostics tdr 1518
interface max-route-limit 1519
interface max-acl-rule-limit <egress/ingress> 1520
interface gigabit-ethernet <port> wred queue <value> min_thresh 1521
interface gigabit-ethernet <port> wred queue <value> max_thresh 1522
interface gigabit-ethernet <port> wred queue <value> enable 1523
interface gigabit-ethernet <port> wred queue <value> ecn_thresh 1524
interface gigabit-ethernet <port> wred queue <value> drop_probability 1525
interface gigabit-ethernet <port> storm-control <mode> ratio <value> 1526
interface gigabit-ethernet <port> storm-control <mode> pps 1527
interface gigabit-ethernet <port> storm-control <mode> kbps 1528
interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id> . . 1529
interface gigabit-ethernet <port> snmp-trap 1530
interface gigabit-ethernet <port> power-preemphasis-level 1531
interface gigabit-ethernet <port> mtu 1532
interface gigabit-ethernet <port> mac-learning <boolean> 1533
interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean> 1534
interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean> 1535
interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged 1536
interface gigabit-ethernet <port> family ethernet-switching native-vlan-id 1537
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode 1538
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress 1539
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type 1540
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress 1541
interface gigabit-ethernet <port> disable 1542
interface gigabit-ethernet <port> ether-options flow-control 1543
interface gigabit-ethernet <port> description 1544
interface gigabit-ethernet <port> crossflow local-control 1545
interface gigabit-ethernet <port> crossflow enable 1546

interface gigabit-ethernet <port> backup-port mode 1547
interface gigabit-ethernet <port> backup-port interface 1548
interface gigabit-ethernet <port> backup-port delay 1549
interface ethernet-switching-options mac-table-aging-time 1550
interface ethernet-switching-options buffer queue-limit 1551
interface ecmp max-path 1552
interface cut-through-mode 1553
interface aggregate-ethernet <lag_name> storm-control <mode> pps 1554
interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan 1555
interface aggregate-ethernet <lag_name> snmp-trap 1556
interface aggregate-ethernet <lag_name> mtu 1557
interface aggregate-ethernet <lag_name> hash-mapping mode 1558
interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id 1559
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode 1560
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress 1561
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type 1562
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress 1563
interface aggregate-ethernet <lag_name> crossflow local-control 1564
interface aggregate-ethernet <lag_name> crossflow enable 1565
interface aggregate-ethernet <lag_name> backup-port mode 1566
interface aggregate-ethernet <lag_name> backup-port interface 1567
interface aggregate-ethernet <lag_name> backup-port delay 1568
interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port 1569
interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control 1570
interface aggregate-balancing hash-mapping field vlan disable 1571
interface aggregate-balancing hash-mapping field port-source disable 1572
interface aggregate-balancing hash-mapping field port-destination disable 1573
interface aggregate-balancing hash-mapping field ip-source disable 1574
interface aggregate-balancing hash-mapping field ip-protocol disable 1575
interface aggregate-balancing hash-mapping field ip-destination disable 1576
interface aggregate-balancing hash-mapping field ingress-interface disable 1577
interface aggregate-balancing hash-mapping field ethernet-type disable 1578
interface aggregate-balancing hash-mapping field ethernet-source-address disable 1579
interface aggregate-balancing hash-mapping field ethernet-destination-address disable 1580
set interface ecmp hash-mapping randomized-load-balancing 1581
set interface ecmp hash-mapping round-robin-load-balancing 1582
set interface ecmp hash-mapping resilient-load-balancing 1583
set interface ecmp hash-mapping dlb-normal 1584
set interface ecmp hash-mapping symmetric 1585
set interface ecmp hash-mapping dlb-optimal 1586
set interface ecmp hash-mapping dlb-assigned 1587
set interface gigabit-ethernet breakout 1588
set interface gigabit-ethernet cdr 1590
VLAN Configuration Commands 1591
set vlans dot1q-tunneling egress from 1592

set vlans dot1q-tunneling egress then action . . . 1593
set vlans dot1q-tunneling egress then service-vlan . . . 1594
set vlans dot1q-tunneling ingress from double-tag service-vlan . . . 1595
set vlans dot1q-tunneling ingress from one-tag customer-vlan-list . . . 1596
set vlans dot1q-tunneling ingress from untag enabled . . . 1597
set vlans dot1q-tunneling ingress then . . . 1598
set vlans vlan-id . . . 1599
set vlans vlan-id description . . . 1600
set vlans vlan-id l3-interface . . . 1601
set vlans vlan-id vlan-name . . . 1602
set vlans vlan-id private-vlan mode . . . 1603
set vlans vlan-id private-vlan association . . . 1604
set mac-map mac-address vlan . . . 1605
run show vlans . . . 1606
run show vlans private-vlan . . . 1607
run show vlans private-vlan type . . . 1608
run show mac-map . . . 1609
set tracemac disable . . . 1610
tracemac . . . 1611
Voice VLAN Configuration Commands . . . 1612
set interface gigabit-ethernet voice-vlan mode . . . 1613
set interface gigabit-ethernet voice-vlan tagged mode . . . 1614
set interface gigabit-ethernet voice-vlan vlan-id . . . 1615
set vlans voice-vlan aging . . . 1616
set vlans voice-vlan dscp . . . 1617
set vlans voice-vlan local-priority . . . 1618
set vlans voice-vlan mac-address mask . . . 1619
set vlans voice-vlan mac-address description . . . 1620
show vlans voice-vlan . . . 1621
show vlans voice-vlan oui . . . 1623
show vlans voice-vlan vlan-id <text> . . . 1624
Layer 3 Routing Commands . . . 1625
run show neighbors . . . 1631
run show route . . . 1632
run show route forward-host . . . 1634
run show route forward-route . . . 1635
run show vrf . . . 1636
set ip vrf . . . 1637
set ip routing enable . . . 1638
set system management-vrf enable . . . 1639
BGP Commands . . . 1640
run show bgp . . . 1642
run show bgp neighbor . . . 1643
run show bgp route . . . 1646
run show bgp unicast neighbor graceful-restart . . . 1647

set protocols bgp aggregate-address . . . 1648
set protocols bgp always-compare-med . . . 1649
set protocols bgp bestpath as-path type multipath-relax . . . 1650
set protocols bgp bestpath bandwidth . . . 1651
set protocols bgp bestpath compare-routerid . . . 1652
set protocols bgp bestpath med missing-as-worst . . . 1653
set protocols bgp cluster-id . . . 1654
set protocols bgp graceful-shutdown . . . 1655
set protocols bgp listen . . . 1656
set protocols bgp local-as . . . 1657
set protocols bgp max-med . . . 1658
set protocols bgp multipath maximum-paths . . . 1659
set protocols bgp neighbor activate . . . 1660
set protocols bgp neighbor addpath-tx-all-paths . . . 1661
set protocols bgp neighbor addpath-tx-bestpath-per-as . . . 1662
set protocols bgp neighbor advertisement-interval . . . 1663
set protocols bgp neighbor allowas-in . . . 1664
set protocols bgp neighbor as-override . . . 1665
set protocols bgp neighbor capability extended-nexthop . . . 1666
set protocols bgp neighbor default-originate . . . 1667
set protocols bgp neighbor description . . . 1668
set protocols bgp neighbor disable-connected-check . . . 1669
set protocols bgp neighbor ebgp-multihop . . . 1670
set protocols bgp neighbor filter-list . . . 1671
set protocols bgp neighbor next-hop-self . . . 1672
set protocols bgp neighbor password . . . 1673
set protocols bgp neighbor peer-group . . . 1674
set protocols bgp neighbor prefix-list . . . 1675
set protocols bgp neighbor remote-as . . . 1676
set protocols bgp neighbor remove-private-as . . . 1677
set protocols bgp neighbor route-map . . . 1678
set protocols bgp neighbor route-reflector-client . . . 1679
set protocols bgp neighbor send-community . . . 1680
set protocols bgp neighbor shutdown . . . 1681
set protocols bgp neighbor soft-reconfiguration . . . 1682
set protocols bgp neighbor timers connect . . . 1683
set protocols bgp neighbor timers holdtime . . . 1684
set protocols bgp neighbor timers keepalive . . . 1685
set protocols bgp neighbor ttl-security hops . . . 1686
set protocols bgp neighbor update-source . . . 1687
set protocols bgp network . . . 1688
set protocols bgp network-import-check . . . 1689
set protocols bgp peer-group . . . 1690
set protocols bgp redistribute . . . 1691
set protocols bgp route-map delay-timer . . . 1692

set protocols bgp router-id 1693
set protocols bgp table-map 1694
set protocols bgp timers 1695
set protocols bgp update-delay 1696
set protocols bgp ebgp-requires-policy 1697
set protocols bgp neighbor timers delayopen 1699
set protocols bgp neighbor maximum-prefix 1700
set protocols bgp neighbor maximum-prefix-out 1701
set protocols bgp neighbor port 1702
set protocols bgp neighbor sender-as-path-loop-detection 1703
set protocols bgp fast-external-failover 1704
set protocols bgp confederation identifier 1705
set protocols bgp confederation peers 1706
set protocols bgp dampening 1707
set protocols bgp default local-preference 1708
set protocols bgp as-notation 1709
set protocols bgp neighbor local-as 1710
OSPFv2 Commands 1711
run clear ospf interface 1713
run show ospf border-routers 1714
run show ospf database 1715
run show ospf interface 1717
run show ospf neighbor 1718
run show ospf route 1719
run show ospf summary-address 1720
set protocols ospf aggregation timer 1721
set protocols ospf area area-type 1722
set protocols ospf area filter-list prefix 1723
set protocols ospf area no-summary 1724
set protocols ospf area range 1725
set protocols ospf area virtual-link 1726
set protocols ospf area virtual-link authentication 1727
set protocols ospf area virtual-link authentication-key 1728
set protocols ospf area virtual-link dead-interval 1729
set protocols ospf area virtual-link hello-interval 1730
set protocols ospf area virtual-link message-digest-key md5 1731
set protocols ospf area virtual-link retransmit-interval 1732
set protocols ospf area virtual-link transmit-delay 1733
set protocols ospf auto-cost reference-bandwidth 1734
set protocols ospf compatible rfc1583 1735
set protocols ospf default-information originate 1736
set protocols ospf default-metric 1737
set protocols ospf interface area 1738
set protocols ospf interface authentication address 1739
set protocols ospf interface authentication message-digest 1740

set protocols ospf interface cost . . . 1741
set protocols ospf interface dead-interval . . . 1742
set protocols ospf interface hello-interval . . . 1743
set protocols ospf interface message-digest-key md5 . . . 1744
set protocols ospf interface network . . . 1745
set protocols ospf interface priority . . . 1746
set protocols ospf interface retransmit-interval . . . 1747
set protocols ospf interface transmit-delay . . . 1748
set protocols ospf log-adjacency-changes . . . 1749
set protocols ospf max-metric router-lsa administrative . . . 1750
set protocols ospf max-metric router-lsa on-shutdown . . . 1752
set protocols ospf max-metric router-lsa on-startup . . . 1754
set protocols ospf multi-instance disable . . . 1756
set protocols ospf network area . . . 1757
set protocols ospf passive-interface . . . 1758
set protocols ospf redistribute . . . 1759
set protocols ospf redistribute metric-type . . . 1760
set protocols ospf redistribute route-map . . . 1761
set protocols ospf router-id . . . 1762
set protocols ospf summary-address . . . 1763
set protocols ospf timers lsa min-arrival . . . 1764
set protocols ospf timers throttle spf . . . 1765
set protocols ospf traceoption ism . . . 1766
set protocols ospf traceoption lsa . . . 1767
set protocols ospf traceoption nsm . . . 1768
set protocols ospf traceoption packet . . . 1769
set protocols ospf traceoption zebra . . . 1770
set protocols ospf graceful-restart enable . . . 1771
set protocols ospf capability opaque . . . 1772
set protocols ospf graceful-restart grace-period . . . 1773
set protocols ospf graceful-restart helper enable . . . 1774
set protocols ospf graceful-restart helper planned-only . . . 1775
set protocols ospf graceful-restart helper strict-lsa-checking . . . 1776
set protocols ospf graceful-restart helper supported-grace-time . . . 1777
run graceful-restart prepare ospf . . . 1778
run show ospf graceful-restart helper . . . 1779
set protocols ospf interface authentication-key . . . 1780
OSPFv3 Command Reference . . . 1781
set protocols ospf6 area . . . 1782
set protocols ospf6 area range . . . 1783
set protocols ospf6 area stub . . . 1784
set protocols ospf6 area stub no-summary . . . 1785
set protocols ospf6 auto-cost reference-bandwidth . . . 1786
set protocols ospf6 distance . . . 1787
set protocols ospf6 distance-ospf6 . . . 1788

set protocols ospf6 interface area . . . 1789
set protocols ospf6 interface cost . . . 1790
set protocols ospf6 interface dead-interval . . . 1791
set protocols ospf6 interface hello-interval . . . 1792
set protocols ospf6 interface ifmtu . . . 1793
set protocols ospf6 interface mtu-ignore . . . 1794
set protocols ospf6 interface network . . . 1795
set protocols ospf6 interface passive . . . 1796
set protocols ospf6 interface priority . . . 1797
set protocols ospf6 interface retransmit-interval . . . 1798
set protocols ospf6 interface transmit-delay . . . 1799
set protocols ospf6 log-adjacency-changes . . . 1800
set protocols ospf6 redistribute . . . 1801
set protocols ospf6 router-id . . . 1802
set protocols ospf6 stub-router administrative . . . 1803
set protocols ospf6 timers lsa min-arrival . . . 1804
set protocols ospf6 timers throttle spf . . . 1805
set protocols ospf6 traceoption . . . 1806
set protocols ospf6 traceoption border-routers . . . 1807
set protocols ospf6 traceoption lsa . . . 1808
set protocols ospf6 traceoption message . . . 1809
set protocols ospf6 traceoption neighbor . . . 1810
set protocols ospf6 traceoption route . . . 1811
set protocols ospf6 traceoption spf . . . 1812
set protocols ospf6 traceoption zebra . . . 1813
set protocols ospf6 graceful-restart enable . . . 1814
set protocols ospf6 capability opaque . . . 1815
set protocols ospf6 graceful-restart grace-period . . . 1816
set protocols ospf6 graceful-restart helper enable . . . 1817
set protocols ospf6 graceful-restart helper planned-only . . . 1818
set protocols ospf6 graceful-restart helper lsa-checking-disable . . . 1819
set protocols ospf6 graceful-restart helper supported-grace-time . . . 1820
run graceful-restart prepare ospf6 . . . 1821
run show ospf6 graceful-restart helper . . . 1822
Static Route Configuration Commands . . . 1823
set protocols static interface-route interface . . . 1824
set protocols static mroute . . . 1825
set protocols static route . . . 1826
Route Map Commands . . . 1827
run show routing route-map . . . 1828
set routing as-path-list . . . 1829
set routing large-community-list expanded . . . 1830
set routing large-community-list standard . . . 1831
set routing prefix-list . . . 1832
set routing prefix-list description . . . 1834

set routing community-list expanded 1835
set routing community-list standard 1836
set routing extcommunity-list expanded 1837
set routing extcommunity-list standard 1838
set routing route-map set-action large-community 1839
set routing route-map call 1840
set routing route-map description 1841
set routing route-map match as-path 1842
set routing route-map match community 1843
set routing route-map match community-with-exact-match 1844
set routing route-map match evpn default-route 1845
set routing route-map match evpn route-type 1846
set routing route-map match evpn vni 1847
set routing route-map match extcommunity 1848
set routing route-map matching-policy 1849
set routing route-map match interface 1850
set routing route-map match ipv4-addr address 1851
set routing route-map match ipv4-addr next-hop 1852
set routing route-map match ipv4-addr route-source 1853
set routing route-map match ipv6-addr 1854
set routing route-map match large-community 1855
set routing route-map match local-preference 1856
set routing route-map match metric 1857
set routing route-map match origin 1858
set routing route-map match peer 1859
set routing route-map match source-protocol 1860
set routing route-map match source-vrf 1861
set routing route-map match tag 1862
set routing route-map on-match 1863
set routing route-map set-action aggregator 1864
set routing route-map set-action as-path exclude 1865
set routing route-map set-action as-path prepend 1866
set routing route-map set-action atomic-aggregate 1867
set routing route-map set-action comm-list-delete 1868
set routing route-map set-action community 1869
set routing route-map set-action community-additive 1870
set routing route-map set-action extcommunity 1871
set routing route-map set-action extcommunity bandwidth 1872
set routing route-map set-action extcommunity bandwidth-non-transitive 1873
set routing route-map set-action ip-next-hop 1874
set routing route-map set-action ipv4-vpn-next-hop 1875
set routing route-map set-action ipv6-next-hop 1876
set routing route-map set-action label-index 1877
set routing route-map set-action large-comm-list-delete 1878
set routing route-map set-action local-preference 1879

set routing route-map set-action metric . . . 1880
set routing route-map set-action metric-type . . . 1881
set routing route-map set-action origin . . . 1882
set routing route-map set-action originator-id . . . 1883
set routing route-map set-action src . . . 1884
set routing route-map set-action tag . . . 1885
set routing route-map set-action weight . . . 1886
Route Leaking Commands . . . 1887
BGP Route Leaking Commands . . . 1888
set protocols bgp ipv4-unicast import vrf . . . 1889
set protocols bgp ipv6-unicast import vrf . . . 1890
set protocols bgp ipv6-unicast import vrf-route-map . . . 1891
set protocols bgp vrf ipv4-unicast import vrf . . . 1892
set protocols bgp vrf ipv4-unicast import vrf-route-map . . . 1893
set protocols bgp vrf ipv6-unicast import vrf . . . 1894
Static Route Leaking Commands . . . 1895
set protocols static route nexthop-vrf next-hop . . . 1896
set protocols static vrf route nexthop-vrf next-hop . . . 1897
BFD Configuration Commands . . . 1898
run show bfd . . . 1899
run show bfd counters . . . 1900
run show bfd peers . . . 1901
set protocols bfd multihop peer local-address . . . 1903
set protocols bfd multihop peer local-address detect-multiplier . . . 1904
set protocols bfd multihop peer local-address minimum-ttl . . . 1905
set protocols bfd multihop peer local-address passive-mode . . . 1906
set protocols bfd multihop peer local-address receive-interval . . . 1907
set protocols bfd multihop peer local-address shutdown . . . 1908
set protocols bfd multihop peer local-address transmit-interval . . . 1909
set protocols bfd peer detect-multiplier . . . 1910
set protocols bfd peer echo-mode . . . 1911
set protocols bfd peer echo receive-interval . . . 1912
set protocols bfd peer echo transmit-interval . . . 1913
set protocols bfd peer local-address . . . 1914
set protocols bfd peer minimum-ttl . . . 1915
set protocols bfd peer passive-mode . . . 1916
set protocols bfd peer receive-interval . . . 1917
set protocols bfd peer shutdown . . . 1918
set protocols bfd peer transmit-interval . . . 1919
set protocols bfd profile . . . 1920
set protocols bfd profile detect-multiplier . . . 1921
set protocols bfd profile echo-mode . . . 1922
set protocols bfd profile echo receive-interval . . . 1923
set protocols bfd profile echo transmit-interval . . . 1924
set protocols bfd profile minimum-ttl . . . 1925

set protocols bfd profile passive-mode . . . 1926
set protocols bfd profile receive-interval . . . 1927
set protocols bfd profile shutdown . . . 1928
set protocols bfd profile transmit-interval . . . 1929
set protocols bgp bfd . . . 1930
set protocols ospf6 interface bfd . . . 1931
set protocols ospf interface bfd . . . 1932
set protocols pim interface bfd . . . 1933
Policy-Based Routing (PBR) Commands . . . 1934
set routing pbr map sequence match destination-ipv4 . . . 1935
set routing pbr map sequence match source-ipv4 . . . 1936
set routing pbr map sequence match destination-port . . . 1937
set routing pbr map sequence match source-port . . . 1938
set routing pbr map sequence match destination-ipv6 . . . 1939
set routing pbr map sequence match source-ipv6 . . . 1940
set routing pbr map sequence action nexthop . . . 1941
set routing pbr map sequence action dscp . . . 1942
set routing pbr map sequence action nexthop-group . . . 1943
set routing nexthop-group nexthop-vrf nexthop . . . 1944
set routing pbr map vlan-interface . . . 1946
run show pbr map . . . 1947
run clear pbr map . . . 1948
IPv4 Source Guard (IPSG for IPv4) Commands . . . 1949
set ip-source-guard binding ip . . . 1950
set ip-source-guard enable . . . 1952
set ip-source-guard verify . . . 1954
set ip-source-guard traceoptions enable . . . 1955
run show ip-source-guard binding . . . 1956
IPv6 Source Guard (IPSG for IPv6) Commands . . . 1957
set ipv6-source-guard binding ip . . . 1958
set ipv6-source-guard enable . . . 1960
set ipv6-source-guard verify . . . 1962
set ipv6-source-guard traceoptions enable . . . 1963
run show ipv6-source-guard binding . . . 1964
ND Inspection Commands . . . 1965
set protocols neighbour inspection vlan disable . . . 1966
set protocols neighbour inspection validate source-mac . . . 1967
set protocols neighbour inspection trust-port . . . 1968
run show nd inspection dhcp6-snooping binding . . . 1969
ND Snooping Commands . . . 1970
set protocols neighbour snooping vlan enable . . . 1971
set protocols neighbour snooping trust-port . . . 1972
set neighbour snooping max-user-number . . . 1973
set protocols neighbour snooping static-prefix vlan . . . 1974
run show neighbor snooping . . . 1975

run show neighbor snooping prefix . . . 1976
run show neighbor snooping binding . . . 1977
run clear neighbor snooping prefix . . . 1978
run clear neighbor snooping binding . . . 1979
IS-IS commands . . . 1980
set protocols isis area-tag network-entity . . . 1982
set protocols isis area-tag is-type . . . 1983
set protocols isis area-tag interface . . . 1984
set protocols isis area-tag hostname-dynamic . . . 1985
set protocols isis area-tag area-password authentication-type . . . 1986
set protocols isis area-tag area-password authentication-key . . . 1987
set protocols isis area-tag area-password authenticate-snp . . . 1988
set protocols isis area-tag domain-password authentication-type . . . 1989
set protocols isis area-tag domain-password authentication-key . . . 1990
set protocols isis area-tag domain-password authenticate-snp . . . 1991
set protocols isis area-tag attached-bit receive-ignore . . . 1992
set protocols isis area-tag attached-bit send . . . 1993
set protocols isis area-tag log-adjacency-changes . . . 1994
set protocols isis area-tag metric-style . . . 1995
set protocols isis area-tag set-overload-bit . . . 1997
set protocols isis area-tag purge-originator . . . 1998
set protocols isis area-tag lsp-mtu . . . 2000
set protocols isis area-tag lsp-timers gen-interval . . . 2001
set protocols isis area-tag lsp-timers refresh-interval . . . 2002
set protocols isis area-tag lsp-timers max-lifetime . . . 2003
set protocols isis area-tag spf-interval . . . 2004
set protocols isis area-tag spf-delay-ietf init-delay . . . 2005
set protocols isis area-tag spf-delay-ietf short-delay . . . 2006
set protocols isis area-tag spf-delay-ietf long-delay . . . 2007
set protocols isis area-tag spf-delay-ietf holddown . . . 2008
set protocols isis area-tag spf-delay-ietf time-to-learn . . . 2009
set protocols isis area-tag default-information originate . . . 2010
set protocols isis area-tag default-information originate metric . . . 2011
set protocols isis area-tag default-information originate route-map . . . 2012
set protocols isis area-tag topology ipv6-unicast . . . 2013
set protocols isis area-tag interface circuit-type . . . 2014
set protocols isis area-tag interface csnp-interval . . . 2015
set protocols isis area-tag interface psnp-interval . . . 2016
set protocols isis area-tag interface hello-padding . . . 2017
set protocols isis area-tag interface hello-interval . . . 2018
set protocols isis area-tag interface hello-multiplier . . . 2019
set protocols isis area-tag interface metric . . . 2020
set protocols isis area-tag interface network point-to-point . . . 2021
set protocols isis area-tag interface passive . . . 2022
set protocols isis area-tag interface password authentication-type . . . 2023

set protocols isis area-tag interface password authentication-key . . . 2024
set protocols isis area-tag interface priority . . . 2025
set protocols isis area-tag interface three-way-handshake . . . 2026
set protocols isis area-tag interface bfd . . . 2027
set protocols isis area-tag interface topology ipv6-unicast . . . 2028
set protocols isis area-tag redistribute . . . 2029
set protocols isis traceoption events . . . 2030
set protocols isis traceoption adj-packets . . . 2031
set protocols isis traceoption route-events . . . 2032
set protocols isis traceoption snp-packets . . . 2033
run show isis summary . . . 2034
run show isis interface . . . 2035
run show isis database . . . 2036
run show isis hostname . . . 2038
run show isis neighbor . . . 2039
run show isis route . . . 2041
run show isis topology . . . 2043
ACL Configuration Commands . . . 2045
set firewall filter description . . . 2046
set firewall filter input interface . . . 2047
set firewall time-range periodic start . . . 2048
set firewall time-range periodic end . . . 2049
run show timerange . . . 2050
run show filter . . . 2051
set firewall filter sequence then dscp . . . 2053
set firewall filter sequence then action . . . 2054
set firewall filter sequence from destination-port . . . 2055
set firewall filter sequence from protocol ip . . . 2056
set firewall filter sequence from protocol ospf . . . 2057
set firewall filter sequence description . . . 2058
set firewall filter output interface . . . 2059
set firewall filter input vlan-interface . . . 2060
set firewall filter sequence from protocol udp . . . 2061
set firewall filter sequence from destination-address-ipv6 . . . 2062
set firewall filter sequence then forwarding-class . . . 2063
set firewall filter sequence from protocol tcp flags . . . 2064
set firewall filter sequence from protocol igmp . . . 2066
set firewall filter output routed-interface . . . 2067
set firewall filter sequence log interval . . . 2068
set firewall filter sequence from source-port . . . 2069
set firewall filter output vlan-interface . . . 2070
set firewall filter sequence from destination-address-ipv4 . . . 2071
set firewall system-output disable . . . 2072
set firewall filter sequence from ip trust-mode . . . 2073
set firewall filter sequence from source-mac-address . . . 2074

set firewall filter sequence from destination-mac-address . . . 2075
set firewall filter sequence from protocol tcp . . . 2076
set firewall filter sequence from ip value . . . 2077
set firewall filter input routed-interface . . . 2078
set firewall filter sequence from protocol icmp . . . 2079
set firewall filter sequence from protocol others . . . 2080
set firewall filter sequence from ether-type . . . 2081
set firewall filter sequence from vlan . . . 2082
set firewall filter sequence from source-address-ipv6 . . . 2083
set firewall filter sequence from source-address-ipv4 . . . 2084
QoS Configuration Commands . . . 2085
set class-of-service forwarding-class local-priority . . . 2087
set class-of-service scheduler mode . . . 2088
set class-of-service interface default-priority . . . 2089
set class-of-service classifier forwarding-class code-point . . . 2091
set class-of-service interface classifier . . . 2092
set class-of-service classifier . . . 2093
set class-of–service classifier forwarding-class . . . 2094
set class-of-service classifier trust-mode . . . 2095
set class-of-service scheduler guaranteed-rate . . . 2096
set class-of-service scheduler-profile forwarding-class scheduler . . . 2097
set class-of-service scheduler weight . . . 2098
set class-of-service easy-ecn mode . . . 2099
set class-of-service interface scheduler-profile . . . 2101
set class-of-service scheduler max-rate . . . 2102
run show class-of-service interface . . . 2103
CoPP Commands . . . 2105
set class-of-service scheduler max-bandwidth-pps . . . 2106
set class-of-service scheduler min-bandwidth-pps . . . 2107
set class-of-service scheduler-profile copp-profile forwarding-classs scheduler . . . 2108
set class-of-service scheduler weight (CoPP) . . . 2109
set firewall filter copp sequence from destination-address-ipv4 . . . 2110
set firewall filter copp sequence from destination-address-ipv6 . . . 2111
set firewall filter copp sequence from destination-mac-address . . . 2112
set firewall filter copp sequence from destination-port . . . 2113
set firewall filter copp sequence from ether-type . . . 2114
set firewall filter copp sequence from protocol . . . 2115
set firewall filter copp sequence from source-address-ipv4 . . . 2116
set firewall filter copp sequence from source-address-ipv6 . . . 2117
set firewall filter copp sequence from source-mac-address . . . 2118
set firewall filter copp sequence from source-port . . . 2119
set firewall filter copp sequence from vlan . . . 2120
set firewall filter copp sequence then forwarding-class . . . 2121
set firewall filter copp sequence then dscp . . . 2122
run show copp bandwidth . . . 2123

run show copp statistics . . . 2124
run show interface stm . . . 2125
run clear copp statistics . . . 2126
set class-of-service forwarding-class local-priority (CoPP) . . . 2127
run show filter copp . . . 2128
Buffer Management Commands . . . 2129
set interface ethernet-switching-options buffer egress-queue shared-ratio . . . 2130
set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared . . . 2131
run show interface egress-buffer . . . 2132
run show interface gigabit-ethernet egress-queues . . . 2133
Interface-based Rate Limiting Commands . . . 2135
set interface gigabit-ethernet rate-limiting ingress kilobits . . . 2136
set interface gigabit-ethernet rate-limiting ingress ratio . . . 2137
set interface gigabit-ethernet rate-limiting ingress burst . . . 2138
set interface gigabit-ethernet rate-limiting egress kilobits . . . 2139
set interface gigabit-ethernet rate-limiting egress ratio . . . 2140
set interface gigabit-ethernet rate-limiting egress burst . . . 2141
ACL-based Traffic Policer Commands . . . 2142
set firewall policer if-exceeding count-mode . . . 2143
set firewall policer if-exceeding rate-limit . . . 2144
set firewall policer if-exceeding burst-limit . . . 2145
set firewall filter sequence then policer . . . 2146
set firewall policer if-exceeding action discard . . . 2147
run show policer . . . 2148
PFC Commands . . . 2149
set class-of-service pfc-profile code-point drop . . . 2150
set class-of-service interface pfc-profile . . . 2152
set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed . . . 2153
set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio . . . 2155
set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold . . . 2156
set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset . . . 2158
set interface ethernet-switching-options buffer service-pool threshold . . . 2160
set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom . . . 2161
set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio . . . 2163
set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold . . . 2164
set class-of-service pfc-watchdog granularity . . . 2166
set class-of-service pfc-watchdog restore-action . . . 2167
set class-of-service pfc-watchdog code-point detect-interval . . . 2168
set class-of-service pfc-watchdog code-point restore-interval . . . 2169
set class-of-service interface pfc-watchdog code-point enable . . . 2170
set class-of-service pfc-watchdog threshold period . . . 2171
set class-of-service pfc-watchdog threshold count . . . 2172
set class-of-service interface pfc-watchdog restore-mode . . . 2173
run clear class-of-service interface pfc-watchdog auto . . . 2175
run clear class-of-service interface pfc-watchdog manual . . . 2176

run show pfc-watchdog stats . . . 2177
run show pfc-watchdog config . . . 2178
run show interface gigabit-ethernet ingress-buffer . . . 2179
run show interface gigabit-ethernet egress-buffer . . . 2180
set class-of-service interface pfc-uplink-group . . . 2181
set class-of-service pfc-uplink-group original-dscp to-code-point . . . 2182
set class-of-service pfc-uplink-group original-dscp dscp . . . 2184
Protocol Configuration Commands . . . 2185
set protocols arp interface address mac-address . . . 2187
set protocols arp interface proxy . . . 2188
set protocols arp inspection vlan disable . . . 2189
set protocols arp inspection access-list ip mac-address . . . 2190
set protocols arp inspection vlan access-list . . . 2191
set protocols arp inspection trust-port . . . 2192
run show arp inspection dhcp-binding . . . 2193
run show arp inspection interface . . . 2194
run show arp inspection vlan . . . 2195
run show arp inspection access-list . . . 2196
run show arp inspection statistics vlan . . . 2197
set protocols arp aging-time . . . 2198
set protocols lacp interface priority . . . 2199
set protocols lacp priority . . . 2200
set protocols sflow agent-id . . . 2201
set protocols sflow collector udp-port . . . 2202
set protocols sflow disable . . . 2203
set protocols dhcp snooping vlan . . . 2204
set protocols dhcp snooping trust-port . . . 2205
set protocols dhcp snooping vlan option82-policy . . . 2206
set protocols dhcp snooping option82 circuit-id . . . 2207
set protocols dhcp snooping option82 remote-id . . . 2208
set protocols dhcp snooping option82 trust-all . . . 2209
set protocols dhcp snooping binding file . . . 2210
set protocols dhcp snooping binding write-delay . . . 2211
run show dhcp snooping binding . . . 2212
set protocols dhcp relay interface disable . . . 2213
set protocols dhcp relay interface dhcp-server-address . . . 2214
set protocols dhcp relay interface relay-agent-address . . . 2215
set protocols dhcp relay interface option82-policy . . . 2216
set protocols dhcp relay option82 circuit-id . . . 2217
set protocols dhcp relay option82 remote-id . . . 2218
set protocols dhcp relay option82 trust-all . . . 2219
set protocols dhcp server pool network . . . 2220
set protocols dhcp server pool range low . . . 2221
set protocols dhcp server pool range high . . . 2222
set protocols dhcp server pool domain-name . . . 2223

set protocols dhcp server pool dns-server . . . 2224
set protocols dhcp server pool default-router . . . 2225
set protocols dhcp server pool lease-time . . . 2226
set protocols dhcp server pool vrf . . . 2227
set protocols dhcp server pool tftp-server . . . 2228
set protocols dhcp server pool log-server . . . 2229
set protocols dhcp server pool bootfile-name . . . 2230
run show dhcp server binding address . . . 2231
run show dhcp server binding interface . . . 2232
set protocols dhcp server interface disable . . . 2233
set protocols dhcp6 relay interface disable . . . 2234
set protocols dhcp6 relay interface destination . . . 2235
set protocols dhcp6 relay interface remote-id . . . 2236
run show dhcp6 relay-stats . . . 2237
set protocols lacp interface rate . . . 2238
run show lldp neighbor . . . 2239
set protocols dhcp6 snooping vlan . . . 2240
set protocols dhcp6 snooping trust-port . . . 2241
set protocols dhcp6 snooping binding file . . . 2242
set protocols dhcp6 snooping binding write-delay . . . 2243
set protocols dhcp6 snooping vlan option-policy . . . 2244
set protocols dhcp6 snooping option37 remote-id . . . 2245
set protocols dhcp6 snooping option18 interface-id . . . 2246
set protocols dhcp6 snooping interface max-clients . . . 2247
run show dhcp6 snooping binding . . . 2248
set protocols dhcp6 guard policy device-role . . . 2249
set protocols dhcp6 guard policy trust-port . . . 2250
set protocols dhcp6 guard policy interface . . . 2251
set protocols dhcp6 guard policy preference-min . . . 2252
set protocols dhcp6 guard policy preference-max . . . 2253
set protocols dhcp6 guard policy match server source-address . . . 2254
set protocols dhcp6 guard policy match reply ia-prefix . . . 2255
run show dhcp6 guard policy . . . 2256
run show dhcp6 guard . . . 2257
run show arp . . . 2258
set protocols sflow interface polling-interval . . . 2260
set protocols sflow header-len . . . 2261
set protocols sflow interface header-len . . . 2262
set protocols sflow interfac sampling-rate egress . . . 2263
set protocols sflow interface disable . . . 2264
set protocols sflow interface sampling-rate ingress . . . 2265
set protocols sflow polling-interval . . . 2266
set protocols sflow sampling-rate egress . . . 2267
set protocols sflow sampling-rate ingress . . . 2268
set protocols sflow source-address . . . 2269

IP Multicast Commands . . . 2270
IGMP Snooping Configuration Commands . . . 2272
run show igmp-snooping . . . 2273
run show igmp-snooping groups . . . 2274
run show igmp-snooping mrouter . . . 2275
run show igmp-snooping querier . . . 2276
set protocols igmp-snooping enable . . . 2277
set protocols igmp-snooping interface max-groups . . . 2278
set protocols igmp-snooping last-member-query-count . . . 2279
set protocols igmp-snooping last-member-query-interval . . . 2280
set protocols igmp-snooping max-response-time . . . 2281
set protocols igmp-snooping query-interval . . . 2282
set protocols igmp-snooping report-suppression . . . 2283
set protocols igmp-snooping robustness-variable . . . 2284
set protocols igmp-snooping vlan-id enable . . . 2285
set protocols igmp-snooping vlan-id fast-leave . . . 2286
set protocols igmp-snooping vlan-id mrouter interface . . . 2287
set protocols igmp-snooping vlan-id querier address . . . 2288
set protocols igmp-snooping vlan-id querier enable . . . 2289
set protocols igmp-snooping vlan-id querier other-querier-timer . . . 2290
set protocols igmp-snooping vlan-id querier version . . . 2291
set protocols igmp-snooping vlan-id static group interface . . . 2292
set protocols igmp-snooping vlan-id unregistered flood-all . . . 2293
IGMP Commands . . . 2294
set protocols igmp interface . . . 2295
set protocols igmp interface join-group . . . 2296
set protocols igmp interface query-interval . . . 2297
set protocols igmp interface query-max-response-time . . . 2298
set protocols igmp interface version . . . 2299
run show igmp groups . . . 2300
run show igmp interface . . . 2301
PIM Configuration Commands . . . 2303
set protocols pim ecmp . . . 2304
set protocols pim interface active-active . . . 2305
set protocols pim interface drpriority . . . 2306
set protocols pim interface hello holdtime . . . 2307
set protocols pim interface hello interval . . . 2308
set protocols pim interface sm . . . 2309
set protocols pim interface use-source . . . 2310
set protocols pim join-prune-interval . . . 2311
set protocols pim keep-alive-timer . . . 2312
set protocols pim packets . . . 2313
set protocols pim register-suppress-time . . . 2314
set protocols pim rp . . . 2315
set protocols pim spt-switchover infinity-and-beyond . . . 2316

set protocols pim ssm prefix-list . . . 2317
set protocols pim interface bsm . . . 2318
set protocols pim interface unicast-bsm . . . 2319
run show pim interface . . . 2321
run show pim rp-info . . . 2322
run show pim neighbor . . . 2323
run show pim upstream . . . 2324
run show mroute . . . 2325
mtrace . . . 2326
run show pim group-type . . . 2327
run show pim bsr . . . 2328
run show pim bsm-database . . . 2329
run show pim bsrp-info . . . 2330
run clear pim bsr-data . . . 2331
Multicast Source Discovery Protocol (MSDP) Commands . . . 2332
set protocols msdp mesh-group source . . . 2333
set protocols msdp mesh-group member . . . 2334
run show msdp mesh-group . . . 2335
run show msdp peer . . . 2336
run show msdp sa . . . 2338
Multicast VLAN Registration (MVR) Commands . . . 2340
run show igmp-snooping mvr mvlan . . . 2341
run show igmp-snooping mvr receiver-vlan . . . 2342
set protocols igmp-snooping vlan-id mvr receiver vlan-list . . . 2343
set protocols igmp-snooping vlan-id mvr source group . . . 2344
OpenFlow Commands in CrossFlow Mode . . . 2345
VXLAN Commands . . . 2346
set vxlans source-interface address . . . 2347
OVSDB VTEP command . . . 2348
set protocols ovsdb controller vrf mgmt-vrf . . . 2349
set protocols ovsdb controller address . . . 2350
set protocols ovsdb controller inactivity-probe-duration . . . 2351
set protocols ovsdb controller maximum-backoff-duration . . . 2352
set protocols ovsdb controller port . . . 2353
set protocols ovsdb controller protocol . . . 2354
set protocols ovsdb interface . . . 2355
set protocols ovsdb management-ip . . . 2356
set protocols ovsdb ssl bootstrap . . . 2357
set protocols ovsdb ssl ca-cert . . . 2358
set protocols ovsdb ssl certificate . . . 2359
set protocols ovsdb ssl private-key . . . 2360
set vxlans l3-vni prefix-routes-only . . . 2361
set vxlans vni mcast-group . . . 2362
run show vxlan statistics . . . 2363
run clear vxlan statistics . . . 2364

set vxlans udp-port . . . 2365
run show vxlan vni . . . 2366
run show vxlan address-table . . . 2367
run show vxlan arp . . . 2368
run show vxlan l3-vni entry . . . 2369
run show vxlan neighbor . . . 2370
set vxlans vni decapsulation mode . . . 2371
set vxlans vni encapsulation mode . . . 2373
set vxlans vni encapsulation vlan . . . 2374
set vxlans vni flood vtep . . . 2375
set vxlans vni flood vtep mac-address . . . 2376
set vxlans vni flood vtep traffic-type . . . 2377
set vxlans vni vlan . . . 2378
set vxlans tunnel-mac-leaning disable . . . 2379
set vxlans l3-vni . . . 2380
BGP EVPN Commands . . . 2381
run show bgp evpn summary . . . 2382
run show bgp evpn import-rt . . . 2383
run show bgp evpn vrf-import-rt . . . 2384
run show bgp evpn vni . . . 2385
run show evpn es . . . 2386
run show evpn access-vlan . . . 2387
run show evpn arp-cache . . . 2389
run show evpn next-hops . . . 2391
run show evpn rmac . . . 2392
run show evpn mac vni . . . 2393
set interface aggregate-ethernet evpn mh es-df-pref . . . 2394
set interface aggregate-ethernet evpn mh es-id . . . 2395
set interface aggregate-ethernet evpn mh es-sys-mac . . . 2396
set l3-interface routed-interface router-mac . . . 2397
set l3-interface vlan-interface anycast address . . . 2398
set l3-interface vlan-interface anycast mac . . . 2399
set l3-interface vlan-interface router-mac . . . 2400
set protocols bgp evpn advertise-default-gw . . . 2401
set protocols bgp evpn advertise ipv4-unicast . . . 2402
set protocols bgp evpn advertise ipv6-unicast . . . 2403
set protocols bgp evpn advertise-svi-ip . . . 2404
set protocols bgp evpn default-originate . . . 2405
set protocols bgp evpn disable-ead-evi-rx . . . 2406
set protocols bgp evpn disable-ead-evi-tx . . . 2407
set protocols bgp evpn vni . . . 2408
set protocols bgp evpn vni advertise-default-gw . . . 2409
set protocols bgp evpn vni advertise-svi-ip . . . 2410
set protocols bgp evpn vni rd . . . 2411
set protocols bgp evpn vni route-target type . . . 2412

set protocols bgp neighbor evpn activate . . . 2413
set protocols bgp neighbor evpn allowas-in . . . 2414
set protocols bgp neighbor evpn route-map . . . 2415
set protocols bgp neighbor evpn route-reflector-client . . . 2416
set protocols bgp vrf evpn advertise-pip ip . . . 2417
set protocols evpn mh mac-holdtime . . . 2418
set protocols evpn mh redirect-off . . . 2419
set protocols evpn mh startup-delay . . . 2420
set vxlans vni arp-nd-suppress disable . . . 2421
set protocols bgp evpn advertise-all-vni . . . 2422
set protocols evpn mh neigh-holdtime . . . 2423
run show bgp evpn route . . . 2424
run show bgp evpn route detail . . . 2426
run show bgp evpn route vni . . . 2428
run show bgp evpn route rd . . . 2430
run show bgp evpn route type . . . 2432
PoE Configuration Commands . . . 2434
set poe interface max-power . . . 2435
set poe interface detection-type . . . 2437
set poe interface enable . . . 2438
set poe interface mode . . . 2439
set poe interface priority . . . 2440
set poe interface threshold-mode . . . 2441
set poe power management-mode . . . 2442
set poe power mode . . . 2443
set poe interface lldp-negotiation . . . 2445
set poe power voltage . . . 2446
set poe traceoptions flag all disable . . . 2447
run show poe interface . . . 2448
run show poe power . . . 2450
set poe perpetual-power enable . . . 2451
VRRP Commands . . . 2453
set protocols vrrp interface vrid . . . 2454
set protocols vrrp interface vrid disable . . . 2455
set protocols vrrp interface vrid version . . . 2456
set protocols vrrp interface vrid ip . . . 2457
set protocols vrrp interface vrid priority . . . 2458
set protocols vrrp interface vrid interval . . . 2459
set protocols vrrp interface vrid preempt enable . . . 2460
set protocols vrrp interface vrid load-balance disable . . . 2461
set protocols vrrp interface vrid load-balance virtual-mac time-interval . . . 2462
set protocols vrrp interface vrid accept disable . . . 2463
set protocols vrrp interface vrid authentication type . . . 2464
set protocols vrrp interface vrid simple-key . . . 2465
set protocols vrrp interface vrid md5-key . . . 2466

run show vrrp . . . 2467
set protocols vrrp interface vrid ipv6-nd adv-interval-option . . . 2468
set protocols vrrp interface vrid ipv6-nd home-agent-config-flag . . . 2469
set protocols vrrp interface vrid ipv6-nd home-agent-lifetime . . . 2470
set protocols vrrp interface vrid ipv6-nd home-agent-preference . . . 2471
set protocols vrrp interface vrid ipv6-nd managed-config-flag . . . 2472
set protocols vrrp interface vrid ipv6-nd mtu . . . 2473
set protocols vrrp interface vrid ipv6-nd other-config-flag . . . 2474
set protocols vrrp interface vrid ipv6-nd prefix off-link . . . 2475
set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime . . . 2476
set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime . . . 2477
set protocols vrrp interface vrid ipv6-nd prefix router-address . . . 2478
set protocols vrrp interface vrid ipv6-nd ra-fast-retrans . . . 2479
set protocols vrrp interface vrid ipv6-nd ra-interval . . . 2480
set protocols vrrp interface vrid ipv6-nd ra-lifetime . . . 2481
set protocols vrrp interface vrid ipv6-nd reachable-time . . . 2482
set protocols vrrp interface vrid ipv6-nd router-preference . . . 2483
set protocols vrrp interface vrid ipv6-nd suppress-ra . . . 2484
Spanning Tree Protocol Commands . . . 2485
run show spanning-tree . . . 2487
run show spanning-tree mstp . . . 2488
run show spanning-tree pvst . . . 2490
run show spanning-tree rstp . . . 2491
run show spanning-tree statistics . . . 2492
run show spanning-tree stp . . . 2493
set protocols spanning-tree enable . . . 2494
set protocols spanning-tree force-version . . . 2495
set protocols spanning-tree interface enable . . . 2496
set protocols spanning-tree mstp bridge-priority . . . 2497
set protocols spanning-tree mstp configuration-name . . . 2498
set protocols spanning-tree mstp forward-delay . . . 2499
set protocols spanning-tree mstp hello-time . . . 2500
set protocols spanning-tree mstp interface bpdu-filter . . . 2501
set protocols spanning-tree mstp interface bpdu-guard . . . 2502
set protocols spanning-tree mstp interface edge . . . 2503
set protocols spanning-tree mstp interface external-path-cost . . . 2504
set protocols spanning-tree mstp interface internal-path-cost . . . 2505
set protocols spanning-tree mstp interface manual-forwarding . . . 2506
set protocols spanning-tree mstp interface mode . . . 2507
set protocols spanning-tree mstp interface port-priority . . . 2508
set protocols spanning-tree mstp interface root-guard . . . 2509
set protocols spanning-tree mstp interface tcn-guard . . . 2510
set protocols spanning-tree mstp max-age . . . 2511
set protocols spanning-tree mstp max-hops . . . 2512
set protocols spanning-tree mstp msti bridge-priority . . . 2513

set protocols spanning-tree mstp msti interface cost . . . 2514
set protocols spanning-tree mstp msti interface port-priority . . . 2515
set protocols spanning-tree mstp revision-level . . . 2516
set protocols spanning-tree mstp msti vlan . . . 2517
set protocols spanning-tree pvst interface bpdu-guard . . . 2518
set protocols spanning-tree pvst interface manual-forwarding . . . 2519
set protocols spanning-tree pvst interface mode . . . 2520
set protocols spanning-tree pvst interface root-guard . . . 2521
set protocols spanning-tree pvst vlan bridge-priority . . . 2522
set protocols spanning-tree pvst vlan enable . . . 2523
set protocols spanning-tree pvst vlan forward-delay . . . 2524
set protocols spanning-tree pvst vlan hello-time . . . 2525
set protocols spanning-tree pvst vlan interface path-cost . . . 2526
set protocols spanning-tree pvst vlan interface port-priority . . . 2527
set protocols spanning-tree pvst vlan max-age . . . 2528
set protocols spanning-tree rstp bridge-priority . . . 2529
set protocols spanning-tree rstp forward-delay . . . 2530
set protocols spanning-tree rstp hello-time . . . 2531
set protocols spanning-tree rstp interface bpdu-filter . . . 2532
set protocols spanning-tree rstp interface bpdu-guard . . . 2533
set protocols spanning-tree rstp interface edge . . . 2534
set protocols spanning-tree rstp interface mode . . . 2535
set protocols spanning-tree rstp interface path-cost . . . 2536
set protocols spanning-tree rstp interface port-priority . . . 2537
set protocols spanning-tree rstp interface root-guard . . . 2538
set protocols spanning-tree rstp interface tcn-guard . . . 2539
set protocols spanning-tree rstp max-age . . . 2540
set protocols spanning-tree stp bridge-priority . . . 2541
set protocols spanning-tree stp forward-delay . . . 2542
set protocols spanning-tree stp hello-time . . . 2543
set protocols spanning-tree stp interface bpdu-filter . . . 2544
set protocols spanning-tree stp interface bpdu-guard . . . 2545
set protocols spanning-tree stp interface edge . . . 2546
set protocols spanning-tree stp interface mode . . . 2547
set protocols spanning-tree stp interface path-cost . . . 2548
set protocols spanning-tree stp interface port-priority . . . 2549
set protocols spanning-tree stp interface root-guard . . . 2550
set protocols spanning-tree stp interface tcn-guard . . . 2551
set protocols spanning-tree stp max-age . . . 2552
MLAG Commands . . . 2553
set protocols mlag domain . . . 2554
set protocols mlag domain node . . . 2555
set protocols mlag domain interface link . . . 2556
set protocols mlag domain peer-ip peer-link . . . 2557
set protocols mlag domain peer-ip peer-vlan . . . 2558

run show mlag domain . . . 2559
run show mlag link . . . 2560
run show mlag consistency-parameter . . . 2561
GRE Tunnel Interface Commands . . . 2563
run show l3-interface tunnel . . . 2564
set l3-interface tunnel address . . . 2565
set l3-interface tunnel destination . . . 2566
set l3-interface tunnel disable . . . 2567
set l3-interface tunnel source . . . 2568
set l3-interface tunnel tunnel-mode gre-ip . . . 2569
set l3-interface tunnel vrf . . . 2570
GVRP Commands . . . 2571
set protocols gvrp join-timer . . . 2572
set protocols gvrp leave-timer . . . 2573
set protocols gvrp leaveall-timer . . . 2574
run clear gvrp interface statistics . . . 2575
run show gvrp interface . . . 2576
run show gvrp interface statistics . . . 2577
set protocols gvrp edge-switch . . . 2578
set protocols gvrp enable . . . 2579
set protocols gvrp interface enable . . . 2580
set protocols gvrp traceoptions flag config . . . 2581
set protocols gvrp traceoptions flag packets . . . 2582
MVRP Commands . . . 2583
run clear mvrp interface statistics . . . 2584
run show mvrp interface . . . 2585
run show mvrp interface statistics . . . 2586
set protocols mvrp edge-switch . . . 2587
set protocols mvrp enable . . . 2588
set protocols mvrp interface enable . . . 2589
set protocols mvrp traceoptions flag config . . . 2590
set protocols mvrp traceoptions flag packets . . . 2591
set protocols mvrp join-timer . . . 2592
set protocols mvrp leave-timer . . . 2593
set protocols mvrp leaveall-timer . . . 2594
ERPS Commands . . . 2595
run show erps brief . . . 2596
run show erps interface . . . 2597
run show erps ring . . . 2598
run show erps statistics . . . 2600
set protocols erps ring . . . 2601
set protocols erps version . . . 2602
set protocols erps enable . . . 2603
set protocols erps ring instance . . . 2604
set protocols erps ring instance control-vlan . . . 2605

set protocols erps ring instance description . . . 2606
set protocols erps ring instance enable . . . 2607
set protocols erps ring instance guard-timer . . . 2608
set protocols erps ring instance holdoff-timer . . . 2609
set protocols erps ring instance protected-instance . . . 2610
set protocols erps ring instance r-aps level . . . 2611
set protocols erps ring instance rpl . . . 2612
set protocols erps ring instance wtr-timer . . . 2613
set protocols erps ring port0 interface . . . 2614
set protocols erps ring port1 interface . . . 2615
set protocols erps ring r-aps ring-mac . . . 2616
set protocols erps ring sub-ring . . . 2617
set protocols erps ring virtual-channel . . . 2618
set protocols erps ring instance non-revertive . . . 2619
set protocols erps tcn-propagation . . . 2620
set protocols erps ring instance connect ring . . . 2621
erps switch force ring instance . . . 2622
erps switch manual ring instance . . . 2623
erps clear ring ring instance . . . 2624
set protocols erps traceoptions flag all disable . . . 2625
set protocols erps traceoptions flag config disable . . . 2626
set protocols erps traceoptions flag ring disable . . . 2627
EFM OAM Commands . . . 2628
set protocols ethernet-oam interface enable . . . 2629
set protocols ethernet-oam interface mode . . . 2630
set protocols ethernet-oam interface remote-loopback supported . . . 2631
set protocols ethernet-oam interface remote-loopback timeout . . . 2632
ethernet-oam remote-loopback start|stop interface . . . 2633
set protocols ethernet-oam interface timeout . . . 2635
set protocols ethernet-oam traceoptions flag packets . . . 2636
set protocols ethernet-oam traceoptions flag config . . . 2637
run show ethernet-oam . . . 2638
run show ethernet-oam statistics . . . 2640
MPLS Commands . . . 2641
set protocols mpls interface . . . 2642
set protocols mpls ldp router-id . . . 2643
set protocols mpls ldp ordered-control . . . 2644
set protocols mpls ldp neighbor password . . . 2645
set protocols mpls ldp neighbor session-holdtime . . . 2646
set protocols mpls ldp neighbor ttl-security disable . . . 2647
set protocols mpls ldp neighbor ttl-security hops . . . 2648
set protocols mpls ldp interface . . . 2649
set protocols mpls ldp ttl-security disable (IP family) . . . 2650
set protocols mpls ldp label-local-advertise . . . 2651
set protocols mpls ldp label-local-allocate . . . 2652

set protocols mpls ldp discovery transport-address . . . 2653
set protocols mpls ldp discovery hello-interval . . . 2654
set protocols mpls ldp discovery hello-holdtime . . . 2655
set protocols mpls ldp discovery targeted-hello-interval . . . 2656
set protocols mpls ldp discovery targeted-hello-holdtime . . . 2657
set protocols mpls ldp discovery targeted-hello-accept . . . 2658
set protocols mpls ldp dual-stack transport-connection prefer-ipv4 . . . 2659
set protocols mpls ldp dual-stack interop . . . 2660
set protocols mpls ldp targeted-neighbor . . . 2661
set protocols mpls ldp traceoption labels . . . 2662
set protocols mpls ldp traceoption errors . . . 2663
set protocols mpls ldp traceoption event . . . 2664
set protocols mpls ldp traceoption discovery . . . 2665
set protocols mpls ldp traceoption messages . . . 2666
run show mpls ldp binding . . . 2667
run show mpls ldp neighbor . . . 2668
run show mpls ldp interface . . . 2672
run show mpls forward-table . . . 2673
run show mpls egress interface . . . 2675
run show mpls table . . . 2676
run show mpls interface . . . 2677
run show mpls status . . . 2678
run show mpls label . . . 2679
run show mpls ldp discovery . . . 2680
run show mpls fec . . . 2681
Loopback Detection Commands . . . 2682
set protocols loopback-detection enable . . . 2683
set protocols loopback-detection interface enable . . . 2684
set protocols loopback-detection message-interval . . . 2685
set protocols loopback-detection traceoptions configuration disable . . . 2686
set protocols loopback-detection traceoptions all disable . . . 2687
run show loopback-detection . . . 2688
run clear loopback-detection interface . . . 2689

PICOS Routing and Switching Configuration Guide

Pica8 PicOS supports Layer 2 switching protocols, including: STP, RSTP, MSTP, MAC learning, and Q-in-Q. PicOS also supports several Layer 3 protocols, including: static routing, RIPv2, OSPF, IGMP, PIM-SM, and IPv6. This guide provides instructions and examples for configuring switches and controllers. Intended for system administrators, this guide assumes a working knowledge of Layer 2 and Layer 3 protocols.

PicOS can run in 2 different modes of operation:

- **Open vSwitch (OVS) Mode:** In this mode, PicOS is dedicated and optimized for OpenFlow applications.
- **Layer 2/Layer 3 (L2/L3) Mode:** In this mode, PicOS can run switching and routing protocols, as well as OpenFlow applications.

In OVS mode, L2/L3 daemons are not running, and the system is fully dedicated to OpenFlow and OVS. In L2/L3 mode, L2/L3 daemons are running, and OVS can also be used if OpenFlow in Crossflow Mode is activated.

This chapter assumes that user is running PicOS L2/L3 mode. Please see PICOS Mode Selection to learn how to switch between L2/L3 and OVS modes.

> **Warning:**
> On FS S5810 Series and S5860 Series switches, run "copy running-config startup-config" command when set L2 / L3 CLI commands. Otherwise, the L2 / L3 configuration will be lost after PicOS reboot. For detail, please refer to Configuration Saving Guide.

PICOS Supported Features

Collection of Feature Specification of Different Platforms

Command-Line Interface

- From Linux Shell to L2/L3 Shell
- Operation Mode and Configuration Mode
- Displaying the Current Configuration
- Display Setting Configuration
- Rolling Back a Configuration
- Managing Configuration Files
- Saving and Loading Configuration Files
- Commit Confirmed
- Commit Check
- Commit Failed and Exit Discard
- Configuring a Command Alias
- Configure L2/L3 from Linux Shell
- Bash Linux Shell
- PicOS Upgrade and Configuration Change
- Set CLI
- CLI Configuration
- Configuring Multi-window Command Configuration Display on The User Terminal
- Configuration Saving Guide

System Administration

- Configuring Management Interface
  - In-Band Management Interface
    - Configuring In-Band Management Interface
    - Default Settings for In-Band Management Interface on S3410 Series Switches
  - Out-of-band Management Interface
    - Configuring Port Speed of eth0 Out-of-Band Management Interface
    - Default Settings for Out-of-band Management Interface
- Configuring User Account and Login Banner
- Configuring SSH and Telnet Parameters
- Configuring the Log-in ACL
- AAA Configuration Guide
  - Introduction
  - Configuration Notes of AAA
  - TACACS+ Configuration
  - RADIUS Configuration
  - Local Authentication Configuration
  - Sample configuration file on the AAA server
- NAC Configuration Guide
  - Configuration Notes of NAC
  - Configuring NAC
  - Configuration Example of NAC
    - Example for Configuring 802.1X Authentication
    - Example for Configuring MAB Authentication
    - Example for Configuring CWA Authentication

        - Example for Configuring Multiple Authentication Modes
    - Typical Configuration of NAC
        - Example for Configuring NAC (PacketFence as the Authentication Server)
        - Solution Documents Download
    - References
    - Principle of NAC
- Configuring NTP and the Time Zone Parameter
- Configuring PTP
- Configuring the linux-config-unreliable
- Configuring IPFIX
- Configuring sFlow
- Configuring the Syslog Log Level
- Configuring the Syslog Disk and Syslog Server
- Displaying System Information
- IPv6 Management Support
- Configuring NETCONF
- SNMP Configuration
    - Configuring SNMPv2
    - Configuring SNMPv3
    - Configuring SNMP ACL
    - Pica8 Private MIB
        - pica_private_mib.my
        - pica_private_trap_mib.my
    - Pica8 Public MIB
    - SNMP Monitoring and Integration with Zabbix
- PoE Configuration Guide
    - Configuring PoE
    - PoE over LLDP Power Negotiation
    - UPoE
    - Configuring Perpetual PoE
- Configuring USB Disable
- Configuring CPU Usage Alarm Threshold
- Configuring MAC Usage Alarm Threshold
- Mirror Configuration
    - Introduction of Mirroring
    - Configuration Notes of Mirroring
    - Configuring Mirror
    - Example for Configuring Local Port Mirroring
    - Example for Configuring ERSPAN
    - Example for Configuring ACL-based ERSPAN
- Configuring gNMI-gRPC Based Telemetry Technology
- Remote Network Monitoring (RMON)
    - Overview of RMON
    - Configuring RMON
    - Example for Configuring RMON
- RESTCONF Configuration
    - Introduction of RESTCONF
    - RESTCONF Operation Methods
    - Configuring RESTCONF
- EFM OAM Configuration
    - Introduction of EFM OAM
    - Configuring EFM OAM
- Configure Telnet to Access to the Remote Device

Interface Management Configuration Guide

- Ethernet Ports Management Configuration
    - Port Naming Conventions
    - Physical Ethernet Port Configuration
    - Configuring Port Breakout and Merge
        - Overview of Port Breakout
        - 100GE and 40GE
        - 400GE and 200GE
        - 800GE
    - Interface Rate Configuraion
        - Introduction of Interface Rate
        - Configuring the Force Rate of an Interface
        - Configuring the Auto-Negotiation Mode
    - Port Security Configuration
    - CDR Function Configuration
    - Time Domain Reflectometry (TDR)
    - Configuring Port Mapping On S4148 Series Switch
    - 10G-Base-KR Interface Configuration

        - Forwarding Error Correction (FEC)
    - Configuring the Loopback Interface
    - Layer 3 VLAN Interface Configuration
    - Configuring Routed Interface
        - Introduction of Routed Interface
        - Configuration Notes of Routed Interface
        - Configuring Routed Interface and Sub-interface
        - Example for Configuring Routed Interface
    - Uplink Failure Detection

Layer 2 Switching Configuration

    - Static MAC entries and Dynamic MAC Address Learning
    - Cut-Through Switching Method
    - MLAG Configuration
        - Principle of MLAG
        - Configuration Notes and Constraints
        - Configuring MLAG
        - Configuration Example of MLAG
            - Example for Configuring a Basic MLAG
            - Example for Configuring MLAG with Active-Active-VRRP
            - Example for Configuring MLAG with DHCP Relay
            - Example for Configuring MLAG with DHCP Snooping
            - Example for Configuring MLAG with IGMP Snooping
            - Example for Configuring MLAG with Rapid PVST+
            - Example for Configuring MLAG with VXLAN
        - MLAG Maintenance and Troubleshooting
            - How to bind a LAG interface to the MLAG link?
            - How to check whether the VLAN configuration on the two peer-link ports are consistent?
            - How to confirm whether the MAC address table has been correctly synchronized?
            - How to enable MLAG traceoptions
            - How to ensure the reliability of the peer link?
            - How to verify configurations on MLAG peer are consistent?
            - How to verify MLAG link status?
            - How to verify MLAG neighbor status?
            - How to verify that the peer link connection status is normal?
            - How to view and clear MLAG statistics?
    - VLAN Configuration
        - Configuring MAC-based VLAN
        - MAC Trace
        - Configuring Port-based VLAN
    - GVRP
        - Overview of GVRP
        - Configuring GVRP
        - Example for Configuring GVRP
    - MVRP
        - Overview of MVRP
        - Configuring MVRP
        - Example for Configuring MVRP
    - Q-in-Q Basic Port Configuration
    - Private VLAN Configuration Guide
        - Introduction of PVLAN
        - Configuration Notes of PVLAN
        - Configuring PVLAN
        - Example for Configuring PVLAN
        - Example for Configuring DHCP Snooping with PVLAN
    - Voice VLAN Configuration Guide
        - Principle of Voice VLAN
        - Configuration Notes of Voice VLAN
        - Configuring Voice VLAN
        - Configuration Example of Voice VLAN
    - Link Aggregation Configuration
        - Static Link Aggregation (LAG) Configuration
        - Link Aggregation Control Protocol (LACP) Configuration
        - LAG Hashing Configuration
            - LAG Hashing Configuration and Example
            - LAG Hash Mapping
            - Resilient LAG Hashing Configuration and Example
        - LACP Fallback
        - Configuring LACP Fast Rate
        - LAG Specification of Different Platforms
    - Symmetric Hash for LAG Configuration Example
    - LLDP Configuration (Link Layer Discovery Protocol)

- LLDP MED Configuration
- MSTP Configuration
- MSTP Configuration Example
- Rapid PVST+ Configuration
- Rapid PVST+ Configuration Example
- BPDU Tunneling Configuration
- UDLD Configuration
- LFS Configuration
- Storm Control in Ethernet Port Configuration
- Ethernet Ring Protection Switching (ERPS)
  - Overview of ERPS
  - Configuration Notes and Constraints of ERPS
  - Configuring ERPS
  - Example for Configuring ERPS (Single Ring)
  - Example for Configuring ERPS (Intersection Rings)
- Loopback Detection
  - Overview of Loopback Detection
  - Configuring Loopback Detection

Layer 3 Routing Configuration

- ARP Configuration
  - Flushing ARP and the Neighbor Table
  - Configuring ARP
  - Dynamic ARP Inspection (DAI)
- Configuring IP Routing
- Static Routing Configuration
  - Configuring Static Routes
  - Example for Configuring IPv4 Static Routes
- VRF Configuration Guide
  - Introduction to VRF
  - Configuration Notes of VRF
  - Configuring a User-defined VRF
  - Enabling Management VRF
  - Example for Configuring Basic VRF
- DHCP Configuration
  - Introduction to DHCP
  - Configuration Notes of DHCP
  - Configuring DHCP Server (IPv4)
  - Configuring DHCP Relay
    - Configuring DHCP Relay (IPv4)
    - Example for Configuring DHCPv6 Relay
    - Example for Configuring DHCP Relay over GRE Tunnel
  - Configuring DHCP Snooping
    - Configuring DHCP Snooping (IPv4)
    - Configuring DHCPv6 Snooping (IPv6)
  - Typical Configuration Example for DHCP Relay and DHCP Snooping
  - DHCPv6 Guard Configuration
    - Overview of DHCPv6 Guard
    - Configuring DHCPv6 Guard
    - Example for Configuring DHCPv6 Guard
  - RFC Lists
- Default Administrative Distance Values
- OSPF (Open Shortest Path First)
  - OSPF Overview
  - Basic OSPF Configuration Tasks
  - Configuring OSPF Route Summarization
  - Basic OSPF Configuration Example
  - OSPF Area Type Configuration Example: NSSA, Stub and Standard Areas
  - OSPF Stub and NSSA Areas with no-summary
  - OSPF Area Range Configuration Guide
  - OSPF Route Redistribution and Route Maps
  - Example for Configuring OSPF with Different VRFs
  - OSPFv3 Configuration Guide
  - OSPF Multi-Instance Support
  - OSPF GR
- ECMP (Equal-Cost Multipath Routing) Configuration
- Symmetric Hash for ECMP Configuration Example
- VRRP Configuration
  - Principle of VRRP
  - Configuration Notes of VRRP
  - Configuring Standard VRRP
  - Configuring Active-Active VRRP

        - VRRP Configuration Example
            - Example for Configuring Standard VRRPv3 for IPv4
            - Example for Configuring Active-Active VRRPv3 for IPv4
            - Example for Configuring Active-Active VRRPv3 for IPv6
- IPv4/IPv6 BGP Configuration
    - BGP Introduction
    - BGP Regular Expressions
    - Basic BGP Configuration
    - Configuring BGP Security
    - Configuring a BGP Route Reflector
    - Configuring BGP Timers
    - Configuring BGP Route Aggregation
    - Configuring BGP Dynamic Neighbors
    - Configuring eBGP Multihop
    - Configuring Removing and Replacing Private ASNs from the AS Path
    - Configuring BGP Multipath
    - Configuring ebgp-requires-policy
    - Enable BGP Read-only Mode
    - Configuring Route Maps for Route Updates
    - BGP Unnumbered
        - Overview of BGP Unnumbered
        - Example for Configuring Basic BGP Unnumbered
        - Example for Configuring BGP Unnumbered EVPN Fabric
    - Configuring BGP Attribute
        - Configuring the AS_Path Attribute
        - Configuring the BGP Community Attribute
        - Configuring the MED Attribute
        - Configuring the Next_Hop Attribute
    - Configuration Examples
        - Example for Configuring Basic BGP Functions
        - Example for Configuring a BGP Route Reflector
        - Example for Configuring BGP Load Balancing
- Routing Map Configuration
    - Routing Map Introduction
    - Configuring Filters
        - Configuring a Community Filter
        - Configuring a Large Community Filter
        - Configuring an AS_Path Filter
        - Configuring an Extended Community Filter
        - Configuring an IP Prefix List
    - Configuring a Routing Map
    - Example for Filtering the Routes to Be Advertised and Receiving
- IPv6 Support
    - IPv6 Neighbor Discovery Configuration
    - PICOS L2/L3 Support for IPv6
    - Enable Path MTU Discovery
- IPv6 Neighbor Discovery Inspection
    - Overview of ND Inspection
    - Configuring ND Inspection
    - Example for ND Inspection
- IPv6 Neighbor Discovery Snooping
    - Overview of ND Snooping
    - Operation Mechanism of ND Snooping
    - Configuring ND Snooping
    - Example for ND Snooping
- VRF Route Leaking Configuration
    - BGP Route Leaking Configuration Example
    - Static Route Leaking Example
- Bidirectional Forwarding Detection (BFD)
    - Introduction of BFD
    - Configuring BFD
        - Configuring Static BFD
        - Configuring Dynamic BFD
    - Configuration Examples of BFD
        - Example for Configuring Single-Hop BFD
        - Example for Configuring Multi-Hop BFD
        - Example for Configuring BFD for BGP
        - Example for Configuring BFD for OSPF
        - Example for Configuring BFD for PIM-SM
    - RFC Lists for BFD
- RIP/RIPng Configuration
    - RIP/RIPng Overview
    - Enabling RIP/RIPng

        - Configuring RIP Version
        - Configuring RIP Route Redistribute
        - Configuring RIPv2 Authentication
        - Configuring RIP to Advertise Default Routes
        - Example for Configuring Basic RIP
        - Example for Configuring Basic RIPng
        - RFC Lists for RIP/RIPng
    - Policy-Based Routing (PBR)
        - Overview of PBR
        - Configuring Policy-Based Routing
        - Example for Configuring Policy-Based Routing
    - IPv4 Source Guard (IPSG for IPv4)
    - IPv6 Source Guard (IPSG for IPv6)
    - IPv6 RA Guard Configuration
    - IS-IS Configuration
        - IS-IS Overview
        - Configuring IS-IS Basic Function
        - Configuring IS-IS Authentication
        - Configuring LSP Packet Attributes
        - Customizing Routes for IS-IS
        - Configuring IS-IS Timers
            - Configuring the Interval for Sending Hello Messages
            - Configuring the Hello-Multiplier for the Neighbor Holding Time
            - Configuring the Interval for Sending CSNP Messages
            - Configuring the Interval for Sending PSNP Messages
        - Controlling IS-IS Routing Information Exchange
            - Configuring IS-IS Advertising Default Routes
            - Configuring IS-IS Introducing External Routes
        - Adjusting SPF Calculation Time
        - Configuration Examples of IS-IS
            - Basic IS-IS Configuration Example
            - Configuration Example of Interaction Between IS-IS and BGP

IP Multicast Routing Configuration

- IGMP Configuration
- PIM Configuration Guide
    - Introduction of PIM
    - Configuring PIM-SM
    - Example for Configuring PIM-SM
    - Example for Configuring PIM-SSM
    - Example for Configuring PIM over GRE Tunnel
    - RFC List of PIM
    - Example for Configuring Basic PIM-SM
- IGMP Snooping Configuration Guide
    - Introduction to IGMP Snooping
    - Enable Unknown Multicast Traffic Flooding with IGMP Snooping Enabled
    - Configuring IGMP Snooping
    - Example for Configuring Basic IGMP Snooping
    - Example for Configuring IGMP Snooping with IGMP
    - RFC List
- Multicast Source Discovery Protocol (MSDP)
    - Introduction of MSDP
    - Example for Configuring PIM-SM Inter-domain Multicast Using MSDP
    - Example for Configuring Anycast RP
    - RFC Lists of MSDP
- Multicast VLAN Registration (MVR)
    - Overview of MVR
    - Configuration Notes and Constraints of MVR
    - Configuring MVR

ACL Configuration

- Configuring Basic ACL
- Configuring Time Range

QoS Configuration

- Weighted Random Early Detection
    - WRED Overview
    - WRED Configuration Tasks
    - WRED Configuration Example
- QoS Principle
- SP Configuration Example

- QoS Configuration Example
  - Configuring Classifier-based QoS
  - Configuring ACL-based QoS
- PFC Configuration Example
- ACL-based Traffic Policer
- CoPP Configuration Guide
  - Principle
  - Default Settings for CoPP (N2224PX-ON/N2248X-ON/N3208PX-ON)
  - CoPP Configuration
    - Configuration Notes
    - Configuring CoPP
    - Configuration Example
  - Default Settings for CoPP
- Queue-based Rate Limiting
- Interface-based Rate Limiting
  - Configuring Ingress Interface-based Rate Limiting
  - Configuring Egress Interface-based Rate Limiting
- WRR Configuration Example
- Buffer Management
- WFQ Configuration Example

VXLAN Configuration

- VXLAN Base Configuration Example
- VXLAN Routing
  - Cross-Subnet Packet Forwarding Process
  - Example for Configuring VXLAN for Different Subnets
- VXLAN Configuration Guide
- VXLAN ECMP Configuration

BGP EVPN Configuration Guide

- BGP EVPN Route Types
- Anycast Gateway for EVPN Distributed Networks
- EVPN Symmetric Routing Configuration Example
- EVPN Asymmetric Routing Example
- EVPN With NAC Configuration Guide
- EVPN Multihoming Configuration Guide
- EVPN Enhancements
- Introduction to BGP EVPN

Generic Routing Encapsulation Protocol (GRE)

- Overview
- GRE Configuration Example

MPLS Configuration

- MPLS Overview
- Configuration Restrictions and Guidlines
- Basic MPLS LDP Configuration
- (Optional) Configuring MPLS LDP Security
- (Optional) Configuring MPLS LDP Timers
- (Optional) Configuring MPLS LDP to Allocate Labels for Host Routes Only
- (Optional) Configuring MPLS LDP PHP (Penultimate Hop Popping)
- Example for Configuring MPLS LDP
- RFC Lists for MPLS

Lossless Network Configuration

- Lossless Network Introduction
- Application Scenarios
- Key Features of Lossless Network
- Configuring Priority-based Flow Control (PFC)
  - Enabling PFC Function
  - Configuring PFC Buffer
  - Configuring PFC Watchdog
  - Configuring PFC Deadlock Prevention
- Configuring Explicit Congestion Notification (ECN)
- Configuring Easy ECN
- PFC and ECN Statistical Reporting through gRPC
- Configuring Dynamic Load Balancing
- Typical Configuration Example of Lossless Network

OpenFlow in Crossflow Mode

- Crossflow Mode Introduction
- CrossFlow Mode Known Limitations
- Crossflow Basic Configuration
- Configuration Example1 in Crossflow Mode
- Configuration Example2 in Crossflow Mode
- Example for Configuring STM Resource Allocation
- Multi-action in crossflow mode

PICOS Supported Features

NOTE:

MPLS is supported only on **Trident3-X7** platforms, which include the following switches: N8550-48B8C, N8550-32C, N8560-32C, S5232F-ON, S5248F-ON and S5296F-ON.

First Level Feature	Secondary Level	Third Level	S5810 Series	S5860 Series	AS9716-32D N9550-32D	S5870-48T6S-U S5870-48T6S S5870-48T6BC-U S5870-48MX6BC-U S5870-48T6BC	N5850-48S6Q N8550-64C	N8550-48B8C N8550-32C N5850-48X6C N5850-48S6C N8560-32C	S3410 Series	N9600-64OD
System Management	Hardware management of system FAN and PSU	/	√	√	√	√	√	√	√	√
	Syslog management	/	√	√	√	√	√	√	√	√
	Boot diagnose	/	√	√	√	√	√	√	√	√
	Recover default configuration and password	/	√	√	√	√	√	√	√	√
	Zero Touch Provisioning (ZTP)	/	√	√	√	√	√	√	√	√
	System file management	/	√	√	√	√	√	√	√	√
	User management	/	√	√	√	√	√	√	√	√
	Support to	/	√	√	√	√	√	√	√	√

	configure login methods									
	System time management: manual method, NTP	/	√	√	√	√	√	√	√	√
	PTP	/	√	√	√	√	√	√	√	×
	Domain Name System (DNS)	/	√	√	√	√	√	√	√	√
	L2L3 WEB Access Control	/	√	√	×	√	×	×	√	×
Layer 2 Switching Configuration	Ethernet Ports Management Configuration	Enable or disable the Ethernet port.	√	√	√	√	√	√	√	√
		Configuring port speed.	√	√	√	√	√	√	√	√
		MTU	√	√	√	√	√	√	√	√
		Flow control	√	√	√	√	√	√	√	√
		Flow statistics	√	√	√	√	√	√	√	√
		Port breakout	√	√	√	√	√	√	×	√
		Routed Interface and	√	√	√	√	√	√	√	√

		Sub-interface								
		Layer 3 VLAN Interface	√	√	√	√	√	√	√	√
		Storm Control	√	√	×	√	√	√	√	√
		Local loopback	√	√	√	√	√	√	√	√
		Backup port	√	√	√	√	√	√	√	√
		Link Fault Signaling (LFS)	√	√	√	√	√	√	√	√
		Forwarding Error Correction (FEC)	√	√	√	√	√	√	×	√
		Time Domain Reflectometry (TDR)	√	√	√	√	√	√	√	√
		Clock and Data Recovery (CDR)	√	√	√	√	√	√	√	√
	MAC configuration	Static MAC entries and Dynamic MAC	√	√	√	√	√	√	√	√

	Address Learning								
Static Link Aggregation (LAG) Configuration	Static LAG	√	√	√	√	√	√	√	√
	Dynamic LAG (LACP)	√	√	√	√	√	√	√	√
	Load balancing	√	√	√	√	√	√	√	√
	Resilient LAG Hashing	×	×	×	√	√	√	×	√
	Symmetric Hash for LAG	√	√	√	√	√	√	×	√
MLAG	Basic MLAG Support IPV6	√	√	√	√	√	√	√	√
	MLAG Active-Active	√	√	√	√	√	√	√	√
	Load balancing	√	√	√	√	√	√	√	√
	MLAG DHCP Snooping	√	√	√	√	√	√	√	√
	MLAG DHCP relay	√	√	√	√	√	√	√	√

	MLAG IGMP snooping	√	√	√	√	√	√	√	×
	MLAG VxLAN	×	×	×	√	√	√	×	×
	MLAG PVST+	√	√	√	√	√	√	√	√
Port access mode	ACCESS Trunk Hybrid	√	√	√	√	√	√	√	√
VLAN	Port-based VLAN	√	√	√	√	√	√	√	√
	MAC Trace	√	√	√	√	√	√	√	√
	MAC-based VLAN	√	√	×	√	√	√	√	×
VLAN mapping	QinQ	√	√	×	√	√	√	√	×
VLAN registration	GVRP	√	√	√	√	√	√	√	√
	MVRP	√	√	√	√	√	√	√	√
Private VLAN	/	√	√	×	√	√	√	√	×
Voice VLAN	/	√	√	√	√	√	√	√	×
Spanning Tree Protocol	STP	√	√	√	√	√	√	√	√
	RSTP	√	√	√	√	√	√	√	√
	MSTP	√	√	√	√	√	√	√	√
	PVST+	√	√	√	√	√	√	√	√
	BPDU Filter	√	√	√	√	√	√	√	√
	BPDU Root	√	√	√	√	√	√	√	√

		Guard							
		BPDU TCN-Guard	√	√	√	√	√	√	√	√
		BPDU-Guard	√	√	√	√	√	√	√	√
		Edge port	√	√	√	√	√	√	√	√
		Manual forwarding	√	√	√	√	√	√	√	√
	BPDU Tunneling	Layer 2 protocol messages such as CDP, LLDP, LACP and STP are supported and can be transmitted through BPDU tunnels.	√	√	√	√	√	√	√	√
	Ethernet Ring Protection Switching (ERPS)	ERPS v1 ERPS v2	√	√	√	√	√	√	√	√
	Unidirectional Link	/	√	√	√	√	√	√	√	√

	Detection (UDLD)									
	Loopback Detection	/	√	√	√	√	√	√	√	√
IP Service Configuration Guide	IPv4 Basic Configuration	/	√	√	√	√	√	√	√	√
	ARP	Static ARP Dynamic ARP	√	√	√	√	√	√	√	√
		ARP Proxy	√	√	√	√	√	√	√	√
	DHCP	DHCP server and DHCP client	√	√	√	√	√	√	√	√
		DHCP relay and dhcp relay option 82	√	√	√	√	√	√	√	√
		DHCP v6 Relay	√	√	√	√	√	√	√	√
		DHCP snooping DHCP snooping trust-port DHCP snooping option 82	√	√	√	√	√	√	√	√
		DHCP v6 snooping	√	√	√	√	√	√	×	√

	Equal-Cost Multipath Routing (ECMP)	Max path Load balancing Symmetric Randomized Load Balance Round-Robin Load Balance Resilient Load Balancing	√	√	√	√	√	√	×	√
	VRF	Base VRF	√	√	√	√	√	√	×	√
		Management VRF and VRF Route Leaking	√	√	√	√	√	√	×	√
	IPv6	IPv6 DHCP Relay IPv6 NDP IPv6 ECMP Path MTU Discovery	√	√	√	√	√	√	√	√

		RA Guard	√	√	√	√	√	√	√	×
IP Routing Configuration	IP addressing	IPv4 Addressing IPv6 Addressing SVI	√	√	√	√	√	√	√	√
	Static routing	IPv4/IPv6 static routing Multiple nexthop static route	√	√	√	√	√	√	√	√
	RIP	RIP Network RIP VRF RIP timer RIP passive-interface Redistribution of static route, connected route, OSPF 2 route and BGP routes into RIP with route	√	√	√	√	√	√	√	√

		map filtering.								
	RIPng	RIPng Network RIP VRF Redistribution of static route, connected route, OSPF 2 route and BGP routes into RIP with route map filtering.	√	√	√	√	√	√	√	√
	OSPF	Single OSPFv2 instance Single OSPFv2 instance for each VRF OSPFv2 Multiple instances Intra- and inter-area	√	√	√	√	√	√	√	√

routing. Type 1 and 2 external routing. Broadcast and P2P interfaces. Stub areas. Not so stubby areas (NSSA) MD5 Authentication. Redistribution of static route, connected route, RIP route and BGP routes into OSPFv2 with route map filtering. OSPFv2 passiv

		e interface OSPFv2 GR (Graceful Restart)								
	OSPFv3	Single OSPFv3 instance Single OSPFv3 instance for each VRF Intra- and inter-area routing Type 1 and 2 external routing Broadcast and P2P interfaces Stub areas Redistribution of static route, connected route, ripng	√	√	√	√	√	√	√	√

		route and BGP routes into OSPFv3 with route map filtering. OSPFv3 passive interface OSPFv3 GR (Graceful Restart)								
	IPv4/IPv6 BGP	BGP Autonomous Systems BGP Route Selection IBGP and EBGP BGP Multiple Autonomous System BGP Peer group BGP fast-extern	√	√	√	√	√	√	×	√

		al-failover BGP update-source EBGP multihop BGP route-map BGP Multipath BGP Route Aggregation BGP Dynamic Neighbors BGP Security BGP Route Reflector BGP Community BGP Unnumbered Redistribution of static route, connected route, RIP route and												

		OSPF routes into BGP with route map filtering.								
	IPv4/IPv6 IS-IS	Network Entity Title (NET) Enable IS-IS Instance on the Interface IS-IS Switch Level IS-IS Authentication: authentication per interface, area authentication and routing domain authentication IS-IS Overload IS-IS Attach	√	√	√	√	√	√	×	√

ed-bit Priority for Designated Router Election IS-IS Passive Interface IS-IS Hello Interval Hello-Multiplier for the Neighbor Holding Time Interval for Sending CSNP Messages Interval for Sending PSNP Messages Advertise Default Routes Introduce External Route

s Adjusting SPF Calculation Time: spf-interval, spf-delay-ietf init-delay, long-delay, holddown, time-to-learn Configure the Maximum Size of Generated LSPs Configure the Minimum Interval between Regenerating LSP Refresh Period for LSPs Maximum

		Valid Time for the LSPs								
	Route Map	IP Prefix List as-path-list community-list large-community-list Route Map Match Route Map Set Route Map Call	√	√	√	√	√	√	√	√
	PBR (Policy-Based Routing)	/	√	√	√	√	√	√	√	√
Multicast Configuration	IGMP	IGMP v2 query IGMP v3 query	√	√	√	√	√	√	×	√

	PIM	PIM SM Static RP Dynamic RP PIM-SSM PIM over GRE Tunnel	√	√	√	√	√	√	×	√
	MSDP	PIM-SM Inter-domain Multicast Using MSDP Anycast RP	√	√	√	√	√	√	×	√
	Multicast routing	Multicast routing and forwarding	√	√	√	√	√	√	×	√
	Multicast VLAN	Multicast VLAN Registration (MVR)	√	√	√	√	√	√	√	√
	IGMP Snooping	IGMP v2 snooping IGMP v3 snooping mrouter	√	√	√	√	√	√	√	×

		port static group unregistered flood								
VPN	Generic Routing Encapsulation Protocol (GRE)	/	×	×	×	√	√	√	×	√
VXLAN	VXLAN	VXLAN	×	×	×	√	√	√	×	×
	EVPN	BGP EVPN	×	×	√	√	√	√	×	×
High Availability	BFD	Static BFD Dynamic BFD Single-Hop BFD Multi-Hop BFD BFD for BGP BFD for OSPF BFD for PIM-SM	√	√	√	√	√	√	×	√
	Uplink Failure Detection (UFD)	Uplink Failure Detection	√	√	√	√	√	√	√	
	Priority Flow Control (PFC)	/	√	√	√	√	√	√	×	√
	Virtual Router	VRRP Active	√	√	√	√	√	√	√	√

	Redundancy Protocol (VRRP)	- Standby VRRP Active - Active (load-balance) VRRP v2 VRRP v3 preempt mode priority authentication accept mode								
	EFM OAM	OAM link discovery Remote loopback	√	√	√	√	√	√	√	×
MPLS	LDP	MD5 Authentication LDP GTSM LDP Transport Address Ordered Control and Indep	See the above notes for supported models.							×

		endent Control Allocate Labels for Host Routes Only LDP PHP								
Lossless Network	PFC, Priority Flow Control	Enabling PFC	√	√	√	√	√	√	×	√
		PFC Buffer	×	×	√	×	×	√	×	√
	PFC Watchdog	Enable PFC watchdog detect-interval restore-action restore-interval	×	×	√	×	×	√	×	√
	PFC Deadlock Prevention	PFC uplink port group Modify the queue priority and DSCP	×	×	√	×	×	√	×	√
	ECN, Explicit Congestion	Enable WRED Set	√	√	√	√	√	√	√	√

	Notification	the maximum and minimum thresholds Set drop probability Enable ECN								
	Easy ECN	Throughput-First mode Latency-First mode	×	×	√	×	×	√	×	√
	DLB, Dynamic Load Balancing	Normal Mode Optimal Mode Assigned Mode	×	×	√	√	×	√	×	√
Security	AAA	Radius Authentication Radius Authorization Radius Accounting	√	√	√	√	√	√	√	√
		TACACS+ Authe	√	√	√	√	√	√	√	√

		nticati on TACA CS+ Autho rizatio n TACA CS+ Accou nting								
		Cons ole Login OUT-band/I NBAN D Login Local Authe nticati on local authe nticati on fallba ck	√	√	√	√	√	√	√	√
	NAC	802.1 X	√	√	√	√	√	√	√	√
		MAC authe nticati on	√	√	√	√	√	√	√	√
		CWA authe nticati on	√	√	√	√	√	√	√	√
		Web authe nticati on Host Mode Serve r Fail VLAN Block	√	√	√	√	√	√	√	√

		VLAN Dynamic VLAN Fallback to WEB EAP Packet Exchange Redirect URL Change of Authorization (CoA) Downloadable ACL Dynamic ACL session-timeout Re-authentication									
	ACL	Match field: destination-address-ipv4 destination-address-ipv6 destin	√	√	√	√	√	√	√	√	

ation-mac-address

destination-port

ether-type

first-fragment

ip

is-fragment

protocol

source-address-ipv4

source-address-ipv6

source-mac-address

source-port

time-range

vlan

ACL-based Traffic Policer

ACL-based

		QoS ACL-based remarked								
	Port Security	Enable or disable port security	√	√	√	√	√	√	√	√
	DAI	Trust Port ARP Packets Validity Checking User Legitimacy Checking Dynamic ARP Inspection ARP Inspection Access List	√	√	√	√	√	√	√	√
	CoPP	System pre-defined control plane protocols Change the pre-defined CoPP	√	√	√	√	√	√	√	√

		policies System customize-defined control plane protocols								
	IPv4SG (IPv4 Source Guard)	IPv4 Source Guard	√	√	√	√	√	√	√	√
	IPv6SG (IPv6 Source Guard)	IPv6 Source Guard	√	√	√	√	√	√	×	×
	DHCPv6 Guard	/	√	√	√	√	√	√	×	√
	Neighbor Discovery Inspection	Enable ND inspection on a VLAN Validate source-mac	√	√	√	√	√	√	×	×
	Neighbor Discovery Snooping	ND Snooping	√	√	√	√	√	√	×	√
QoS Service Configuration	Queue scheduler	Queue scheduler: SP WRR WFQ	√	√	√	√	√	√	√	√
	Traffic policing	Traffic policing: guara	√	√	√	√	√	√	√	√

		nteed-rate max-rate Traffic classifier								
	Congestion management and avoidance	Congestion management:WRED Congestion avoidance:ECN	√	√	√	√	√	√	√	√
Network Management and Monitoring	SNMP	SNMP v2	√	√	√	√	√	√	√	√
		SNMP v3	√	√	√	√	√	√	√	√
		SNMP Access control SNMP authentication SNMP privacy SNMP Trap SNMP VRF	√	√	√	√	√	√	√	√
	RESTCONF	/	√	√	√	√	√	√	×	√
	Remote Network Monitoring (RMON)	Ethernet statistics function (ether Stats Table	√	√	√	√	√	√	√	√

		in RMON MIB)								
		History statistics function (etherHistoryTable in RMON MIB)	√	√	√	√	√	√	√	√
		Event definition function (eventTable and logTable in RMON MIB)	√	√	√	√	√	√	√	√
		Alarm threshold setting function (alarmTable in RMON MIB)	√	√	√	√	√	√	√	√
	NETCONF	/	√	√	√	√	√	√	×	√
	LLDP	LLDP Mode Selecting	√	√	√	√	√	√	√	√

	Optional TLVs								
	LLDP med	√	√	√	√	√	√	√	√
POE	PoE threshold-mode PoE max-power power management-mode PoE power mode PoE over LLDP Power Negotiation Perpetual PoE	Only supported on devices with 'P' or 'U' in their names.							
Mirror Configuration	Local port mirror	√	√	√	√	√	√	√	√
	ERSPAN	√	x	√	√	√	√	×	√
	Base ACL ERSPAN	√	x	√	√	√	√	×	√
Switch Environment monitor	boot-messages connections cpu-usage fan hwinf	√	√	√	√	√	√	√	√

		o memory-usage processes rollback rpsu serial-number temperature								
	Packet Capture	tcpdump	√	√	√	√	√	√	√	√
	Telemetry Protocol	/	√	√	√	√	√	√	×	√
	SDN	Openflow	√	√	√	√	√	√	×	×
	sFlow	collector udp port source address header length sampling rate	√	√	√	√	√	√	√	×

Collection of Feature Specification of Different Platforms

Specification of some features vary by platform, this page provides a collection of feature specification of different platforms.

- Table 1 The maximum number of LAGs supported by different platforms
- Table 2 The maximum number of member ports per LAG

Table 1 The maximum number of LAGs supported by different platforms

Model	Max Number of LAGs
AS7326-56x	79
AS4610_30p	48
AS4610_54p	54
AS5712_54x	72
AS5812_54x	72
AS5812_54t	72
AS7312_54x	72
AS6701_32x	104
AS6712_32x	104
AS7712_32x	128
AS6812_32x	104
AG5648	72
AG7648	72
S4048	72
Z9100	128
N3248PXE-ON / N3248P-ON	60
S5212F-ON	24
S5224F-ON	40
S5296F-ON	128
*S4148T / S4148F (100G)	64
*S4148T / S4148F (40G)	72
N3224PX-ON	36

*S4148T / S4148F (100G): Indicates that port mapping of the six interfaces of QSFP+ and QSFP28 on the front panel is **4 x 100G**.

*S4148T / S4148F (40G): Indicates that port mapping of the six interfaces of QSFP+ and QSFP28 on the front panel is **6 x 40G**.

The maximum number of member ports per LAG is model dependent, see the table below.

Table 2 The maximum number of member ports per LAG

Model	Max Member Ports per LAG
AS4610_30p	8
AS4610_54p	8
AS5712_54p	64
AS5812_54t	64
AS5812_54x	64
AS6701_32x	64
AS6712_32x	64
AS7712_32x	64

Model	Max Member Ports per LAG
AS7312_54x	64
AS6812_32x	64
AG5648	64
AG7648	64
S4048	64
Z9100	64
N3248PXE-ON / N3248P-ON	64
S5212F-ON	64
S5224F-ON	64
S5296F-ON	64
S4148T / S4148F	64
N3224PX-ON	64

Command-Line Interface

- From Linux Shell to L2/L3 Shell
- Operation Mode and Configuration Mode
- Displaying the Current Configuration
- Display Setting Configuration
- Rolling Back a Configuration
- Managing Configuration Files
- Saving and Loading Configuration Files
- Commit Confirmed
- Commit Check
- Commit Failed and Exit Discard
- Configuring a Command Alias
- Configure L2/L3 from Linux Shell
- Bash Linux Shell
- PicOS Upgrade and Configuration Change
- Set CLI
- CLI Configuration
- Configuring Multi-window Command Configuration Display on The User Terminal
- Configuration Saving Guide

From Linux Shell to L2/L3 Shell

Once in the Linux shell, user can use the command **pica_sh** or **cli** (under /pica/bin) to launch the L2/L3 CLI (or XORP CLI).

```
admin@XorPlus$
admin@XorPlus$cli
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on XorPlus
admin@XorPlus>
```

To come back to the Linux Shell from the L2/L3 CLI (or XORP CLI), use the **exit** command.

```
admin@XorPlus> exit
admin@XorPlus$
```

PICOS go2cli Version

> **NOTE:**
> For PICOS **go2cli** version, the operation is different.

For PICOS **go2cli** version, users go to PICOS CLI prompt after log in:

```
admin@Xorplus>
```

At PICOS CLI prompt, run "**start shell sh**" to enter Linux shell.

```
admin@Xorplus> start shell sh
admin@Xorplus:~$
```

If you want to return from the Linux shell back to the CLI prompt, run "**exit**".

```
admin@Xorplus:~$ exit
exit

admin@Xorplus>
```

Operation Mode and Configuration Mode

By default, the switch's operation mode is activated when it starts up.

Welcome to PicOS L2/L3 on XorPlus

```
admin@XorPlus>
```

Activate the configuration mode by entering the configure command. Be sure to enter the configuration mode if the admin@XorPlus# prompt appears.

```
admin@XorPlus> configure
Entering configuration mode.
There are no other users in configuration mode.
admin@XorPlus#
```

Displaying the Current Configuration

In L2/L3, non-default configuration can be displayed with the **show** commands. The command **show all** displays the default value of the current configuration. Default configurations are shown in the pica_default.boot file. The command **show running-config** displays the configuration active on the system.

```
admin@XorPlus# show
vlans {
vlan-id 200 {
}
}
admin@XorPlus#
admin@XorPlus# show all
vlans {
vlan-id 200 {
description: ""
vlan-name: "default"
l3-interface: ""
}
}
```

```
admin@XorPlus> show running-config
    vlans {
        vlan-id 200 {
        }
    }
```

Display Setting Configuration

This command displays which settings the configuration has set by default and which settings need to set manually.

```
admin@XorPlus# show | display set
set interface ethernet-switching-options analyzer test input ingress ge-1/1/2
set interface ethernet-switching-options analyzer test input egress ge-1/1/2
set interface ethernet-switching-options analyzer test output "ge-1/1/3"
```

```
admin@XorPlus# show | display set
    set vlans vlan-id 11
    set vlans vlan-id 22
admin@XorPlus#
admin@XorPlus# set vlans vlan-id 33
admin@XorPlus# set vlans vlan-id 44
admin@XorPlus# set vlans vlan-id 55
admin@XorPlus# show | display set
    set vlans vlan-id 11
    set vlans vlan-id 22
>   set vlans vlan-id 33
>   set vlans vlan-id 44
>   set vlans vlan-id 55
admin@XorPlus# com
Merging the configuration.
Commit OK.
Save done.
admin@XorPlus# show | display set
    set vlans vlan-id 11
    set vlans vlan-id 22
    set vlans vlan-id 33
    set vlans vlan-id 44
    set vlans vlan-id 55
admin@XorPlus#
```

Rolling Back a Configuration

Each time a configuration in L2/L3 is commited, a rollback configuration file is created. For example, if configuration is committed five times, **pica.conf.01** through **pica.conf.05** are created. User can rollback to any of these configurations when necessary. The maximum quantity of rollback files is limited to five. The current configuration is located in ***pica.conf***.

```
admin@XorPlus# rollback 1
admin@XorPlus# Loading config file...
Config file was loaded successfully.
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Displaying the difference between the current config with destination config file

```
admin@XorPlus# show | compare rollback 2
[edit vlans]
-------------------------------------------------------------------------------------
+vlan-id 3 {
+}
admin@XorPlus#
```

The **rollback default** command completely replaces the running configuration with the default configuration file. After this command is executed, a commit is required to make the rollback to default configuration take effect.

Warning: This command should be used with caution. All the user configurations will be overridden by the default configurations.

Example,

```
admin@Xorplus# show | display set
    set system management-vrf enable true
    set system ntp vrf "mgmt-vrf"
    set system ntp server-ip 10.10.50.143
    set system syslog server-ip 10.10.50.143
    set system syslog vrf "mgmt-vrf"
    set system aaa tacacs-plus key "VzVua2V5c3RyaW5nYTJW"
    set l3-interface loopback lo address 20.1.1.1 prefix-length 32
    set l3-interface vlan-interface vlan100 address 30.1.1.1 prefix-length 24
    set vlans vlan-id 100 l3-interface "vlan100"

admin@Xorplus# rollback default
Loading config file...
Config file was loaded successfully.
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# show | display set

admin@Xorplus#
```

Managing Configuration Files

Configuration files can be copied, deleted, or renamed in the system, but system files should *not* be deleted.

The L2/L3 configuration is stored in /pica/config/pica_startup.boot.

```
admin@XorPlus$
admin@XorPlus$cd /pica/config/
admin@XorPlus$ls
admin  pica.conf  pica.conf.01  pica.conf.02  pica.conf.03  pica.conf.04  pica.conf.05  pica startup.boot root
```

User can display the files of a specified directory:

```
admin@XorPlus> file list /
drwxr-xr-x 2 root xorp 4096 Sep 25 00:54 bin
drwxr-xr-x 2 root xorp 4096 Sep 24 06:21 boot
drwxr-xr-x 2 root xorp 4096 Sep 23 17:05 cftmp
-rwxr-xr-x 1 root xorp 40559 Sep 23 17:05 config.bcm
drwxr-xr-x 4 root root 4096 Sep 25 00:54 dev
drwxr-xr-x 7 root xorp 4096 Sep 25 00:55 etc
drwxr-xr-x 4 root xorp 4096 Sep 24 06:21 lib
lrwxrwxrwx 1 root root 11 Sep 24 06:21 linuxrc -> bin/busybox
drwxr-xr-x 5 root xorp 4096 Sep 24 06:21 mnt
drwxr-xr-x 2 root xorp 4096 Sep 23 17:05 opt
drwxr-xr-x 5 root xorp 4096 Sep 24 06:21 ovs
drwxr-xr-x 14 root xorp 4096 Sep 24 06:23 pica
dr-xr-xr-x 52 root root 0 Jan 1 1970 proc
-rwxr-xr-x 1 root xorp 59012 Sep 23 17:05 rc.soc
drwxr-xr-x 2 root xorp 4096 Sep 24 06:21 sbin
drwxr-xr-x 11 root root 0 Jan 1 1970 sys
drwxrwxrwx 8 root xorp 1024 Sep 25 00:55 tmp
drwxr-xr-x 7 root xorp 4096 Sep 24 06:22 usr
drwxr-xr-x 7 root xorp 4096 Sep 24 06:23 var
admin@XorPlus> file list /tmp
drwxrwxr-x 5 root xorp 1024 Sep 25 00:54 home
drwxrwxr-x 2 root xorp 1024 Sep 25 00:54 log
drwx------ 2 root root 12288 Sep 25 00:54 lost+found
drwxrwxr-x 3 root xorp 1024 Sep 25 00:55 run
drwxrwxr-x 2 root xorp 1024 Sep 25 00:54 snmp
drwxrwxr-x 2 root xorp 1024 Sep 25 00:56 system
```

Display the contents of a specified file:

```
--    1 root     root          410 Sep 24 06:23 boot.lst
-rw-rw-r-- 1 root xorp 16006 Sep 24 07:44 pica.conf
-rw-rw-r-- 1 root xorp 16003 Sep 24 07:22 pica.conf.01
-rw-rw-r-- 1 root xorp 15826 Sep 24 07:19 pica.conf.02
-rw-rw-r--1 root xorp 15536 Sep 24 07:18 pica.conf.03
-rw-rw-r-- 1 root xorp 15915 Sep 24 07:18 pica.conf.04
-rw-rw-r-- 1 root xorp 15567 Sep 24 07:09 pica.conf.05
drwxrwxrwx 2 root root 4096 Sep 24 06:25 root
admin@XorPlus> file show /pica/config/pica.conf
/*XORP Configuration File, v1.0*/
interface {
ecmp {
max-path: 4
hash-mapping {
field {
ingress-interface {
disable: false
}
vlan {
disable: false
}
ip-protocol {
disable: false
}
ip-source {
disable: false
}
ip-destination {
disable: false
}
port-source {
disable: false
}
port-destination {
disable: false
}
}
}
}
}
```

User can also copy, archive, checksum, compare, rename, and sync files.

```
admin@XorPlus> file list /pica/config
-rw-r--r-- 1 root root 410 Sep 24 06:23 boot.lst
-rw-rw-r-- 1 root xorp 16006 Sep 24 07:44 pica.conf
-rw-rw-r-- 1 root xorp 16003 Sep 24 07:22 pica.conf.01
-rw-rw-r-- 1 root xorp 15826 Sep 24 07:19 pica.conf.02
-rw-rw-r-- 1 root xorp 15536 Sep 24 07:18 pica.conf.03
-rw-rw-r-- 1 root xorp 15915 Sep 24 07:18 pica.conf.04
-rw-rw-r-- 1 root xorp 15567 Sep 24 07:09 pica.conf.05
```

```
drwxrwxrwx 2 root root 4096 Sep 24 06:25 root
admin@XorPlus> file copy /pica/config/pica.conf
Possible completions:
<destination-file> Copy files to and from the router
admin@XorPlus> file copy /pica/config/pica.conf /pica/config/ychen.conf
admin@XorPlus> file list /pica/config
-rw-r--r-- 1 root root 410 Sep 24 06:23 boot.lst
-rw-rw-r-- 1 root xorp 16006 Sep 24 07:44 pica.conf
-rw-rw-r-- 1 root xorp 16003 Sep 24 07:22 pica.conf.01
-rw-rw-r-- 1 root xorp 15826 Sep 24 07:19 pica.conf.02
-rw-rw-r-- 1 root xorp 15536 Sep 24 07:18 pica.conf.03
-rw-rw-r-- 1 root xorp 15915 Sep 24 07:18 pica.conf.04
-rw-rw-r-- 1 root xorp 15567 Sep 24 07:09 pica.conf.05
drwxrwxrwx 2 root root 4096 Sep 24 06:25 root
-rw-rw-r-- 1 root root 16006 Sep 25 02:22 ychen.conf
admin@XorPlus>
admin@XorPlus> file rename /pica/config/ychen.conf /pica/config/ychen-1.conf
admin@XorPlus> file list /pica/config
-rw-r--r-- 1 root root 410 Sep 24 06:23 boot.lst
-rw-rw-r-- 1 root xorp 16006 Sep 24 07:44 pica.conf
-rw-rw-r-- 1 root xorp 16003 Sep 24 07:22 pica.conf.01
-rw-rw-r-- 1 root xorp 15826 Sep 24 07:19 pica.conf.02
-rw-rw-r-- 1 root xorp 15536 Sep 24 07:18 pica.conf.03
-rw-rw-r-- 1 root xorp 15915 Sep 24 07:18 pica.conf.04
-rw-rw-r-- 1 root xorp 15567 Sep 24 07:09 pica.conf.05
drwxrwxrwx 2 root root 4096 Sep 24 06:25 root
-rw-rw-r-- 1 root root 16006 Sep 25 02:22 ychen-1.conf
admin@XorPlus>
admin@XorPlus> file checksum /pica/config/ychen-1.conf
3559192236 16006 /pica/config/ychen-1.conf
admin@XorPlus>
admin@XorPlus> file sync
admin@XorPlus>
admin@XorPlus> file compare /pica/config/pica.conf /pica/config/pica.conf.01
admin@XorPlus> file compare /pica/config/pica.conf /pica/config/pica.conf.01
3c3
< /*Last commit     : Mon Jan 13 14:13:01 2014 by admin*/
---
> /*Last commit     : Mon Jan 13 14:12:26 2014 by admin*/
510,514d509
< controller 1 {
< protocol: "tcp"
< address: 10.10.50.47
< port: 6633
< }
```

User can change the current directory using functions like cwd or cd.

```
admin@XorPlus> file cwd
Current working directory: /tmp/home/admin
admin@XorPlus>
admin@XorPlus> file cwd /pica/config
admin@XorPlus> file cwd
Current working directory: /pica/config
admin@XorPlus>
```

Saving and Loading Configuration Files

The Pica8 PicOS provides several commands to save, load, and execute PicOS configuration files, as detailed in this document.

> The **save** command saves configuration files in the */home/admin* directory for admin user, and /home/test directory for test user. The **load** and **execute** commands look for configuration files in the same directory.

You can use the **save** command in L2/L3 configuration mode to save the running configuration to a file. The following example demonstrates how to save the running configuration to a file named *myconfig.conf*.

```
admin@Spine1# save ?
Possible completions:
  <file name>                   Save running configuration to specified file
admin@Spine1# save myconfig.conf
Save done.
```

The configuration saved earlier in a file can be loaded or applied using the **load merge** or **load override** command in L2/L3 mode.

```
admin@Spine1# load ?
Possible completions:
  merge                         Merge the loaded configuration to the current running configuration
  override                      Override the current running configuration with the loaded configuration
```

The **load override** command completely replaces the running configuration with the configuration in a file (saved earlier). The following example replaces the running configuration with the configuration in a file named *myconfig.conf*.

```
admin@Spine1# load override ?
Possible completions:
  <text>                        Local file name
  myconfig.conf                 Size: 16643, Last changed: Wed Sep  9 21:33:21 2015
admin@Spine1# load override myconfig.conf
Loading config file...
Config file was loaded successfully.
```

NOTE:

When you fail to load configuration file by using the **load override** command, you can try using **load merge** command to load the configuration file.

The **load merge** command merges the configuration in a file (saved earlier) with the running configuration. The following example merges the configuration in a file named *myconfig.conf* with the running configuration.

```
admin@Spine1# load merge ?
Possible completions:
  <text>                        Local file name
  myconfig.conf                 Size: 16643, Last changed: Wed Sep  9 21:33:21 2015
admin@Spine1# load merge myconfig.conf
Loading config file...
Config file was applied successfully.
```

Commit Confirmed

User can commit a candidate configuration before this configuration becomes permanent. By using **commit confirmed**, the system will apply the configuration with a ten minute default. After ten minutes, the system will roll back to the original configuration automatically. User can configure the roll back time in the CLI. By default, roll back time is 10 minutes.

By default, it will be automatically rolled back to the previous configuration after 600 seconds (10 minutes).

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# commit confirmed
Merging the configuration.
Will be automatically rolled back in 600 seconds unless confirmed by new commit.
Commit OK.
admin@XorPlus#
```

Modify the rollback confirmation time

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# commit confirmed 100
Merging the configuration.
Will be automatically rolled back in 100 seconds unless confirmed by new commit.
Commit OK.
admin@XorPlus#
```

Commit Check

User can check to see if the configuration is correct before this configuration becomes permanent. Use **commit check**. A result of "Commit check ok" means the configuration is correct as is. Then, user can commit the configuration to become permanent. A result of "Commit check failed" means the configuration has an error that needs to be corrected.

Commit Check one correct configuration

```
admin@XorPlus# set vlans vlan-id 4094
admin@XorPlus# commit check
Commit check OK.
admin@XorPlus#
admin@XorPlus# show all
    vlans {
>       vlan-id 4094 {
>           description: ""
>           vlan-name: "default"
>           l3-interface: ""
>       }
    }
admin@XorPlus#
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# show all
    vlans {
        vlan-id 4094 {
            description: ""
            vlan-name: "default"
            l3-interface: ""
        }
    }
admin@XorPlus# run show vlans
VlanID   Tag        Interfaces
------   --------   ------------------------------------------------------
1        untagged   ge-1/1/1, ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5
                    ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                    ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                    ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                    ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25
                    ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30
                    ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35
                    ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40
                    ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45
                    ge-1/1/46, ge-1/1/47, ge-1/1/48, te-1/1/49, te-1/1/50
                    te-1/1/51, te-1/1/52
         tagged
4094     untagged
         tagged
```

Commit Check one incorrect configuration

```
admin@XorPlus# set vlans vlan-id 4096
admin@XorPlus# commit check
Invalid vlan 4096
Commit check failed.
admin@XorPlus#
admin@XorPlus# show
    vlans {
>       vlan-id 4096 {
>       }
    }
admin@XorPlus# commit
Invalid vlan 4096
Commit failed.
```

```
admin@XorPlus#
admin@XorPlus# exit discard
admin@XorPlus>
admin@XorPlus> configure
```

Commit Failed and Exit Discard

Switch from the configuration mode to the execution mode *without* any uncommitted configurations.

```
admin@XorPlus# exit
admin@XorPlus>
```

Use the exit discard command to enter the execution mode from the configuration mode with any uncommitted or failed committed configurations.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable true
admin@XorPlus# exit
ERROR: There are uncommitted changes.
Use "commit" to commit the changes, or "exit discard" to discard them.
admin@XorPlus# exit discard
admin@XorPlus>
```

Configuring a Command Alias

User can configure an alias for a PicOS command. This CLI also supports multiple parameters. In other words, user can use the parameter in PicOS CLI e.g. $1,$2…., which will be used in the alias command.

```
admin@XorPlus# set alias set_vlans as "set vlans vlan-id $1"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set_vlans 10
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set alias set_vlans_interface as " set vlans vlan-id $1 vlan-name $2"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set_vlans_interface 20 vlan20
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure L2/L3 from Linux Shell

Configure L2/L3 via Linux Shell on PicOS.

```
admin@XorPlus:~$cli -c "configure;set vlans vlan-id 100;commit"
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on XorPlus
admin@XorPlus>
Execute command: configure.
Entering configuration mode.
There are no other users in configuration mode.
admin@XorPlus#
Execute command: set vlans vlan-id 100.
admin@XorPlus#
Execute command: commit
.
The configuration has been changed by user admin
DELTAS:
    vlans {
        vlan-id 100 {
            vlan-name: "default"
        }
    }
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus:~$
```

Show the Configuration via Linux Shell

```
admin@XorPlus:~$cli -c "show vlans"
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on XorPlus
admin@XorPlus>
Execute command: show vlans
.
VlanID   Tag        Interfaces
------   --------   ------------------------------------------------------
1        untagged   ge-1/1/1, ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5
                    ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                    ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                    ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                    ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25
                    ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30
                    ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35
                    ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40
                    ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45
                    ge-1/1/46, ge-1/1/47, ge-1/1/48, te-1/1/49, te-1/1/50
                    te-1/1/51, te-1/1/52
         tagged
100      untagged
         tagged
admin@XorPlus>
admin@XorPlus:~$
```

Bash Linux Shell

User can execute Linux commands in the PicOS CLI to display the system process, create a directory, or execute commands added by third party software.

```
admin@XorPlus# run bash "ps"
  PID TTY          TIME CMD
5289 ttyS0    00:00:00 bash
5301 ttyS0    00:00:03 pica_sh
7725 ttyS0    00:00:00 ps
admin@XorPlus# run bash "pwd"
/home/admin
admin@XorPlus>
```

If the command requires multiple parameters, quotation marks are required. Here is an example from the configuration mode used to check the system configuration file.

```
TelAviv# run bash "cat /pica/config/pica.conf"
/*XORP Configuration File, v1.0*/
/* Copyright (C) 2009-2013 Pica8, Inc.*/
/*Last commit : Fri May 9 12:43:39 2014 by admin*/
/*PicOS Version : 2.3*/
/*Version Checksum: 6b1435290092ce1b89fb98c06e20e66c*/
[...]
```

PicOS Upgrade and Configuration Change

As part of PicOS improvements, the CLI configuration structure may change between releases. Some commands or knobs may be added, removed, or modified. At the same time, a switch should be able to be upgraded without impact to a network, while still keeping the configuration intact.

A process was defined to achieve both of those goals (improved CLI with smooth upgrade).

When a command is modified in a release, the old command is marked with a "deprecated" flag.

A "deprecated" command can still be used on the next PicOS version, and, at a minimum, on all the PicOS versions published during the life time of this version (typically 9 months for a standard release).

Deprecated commands are hidden from the CLI, so a new user cannot access it without specific knowledge of the command (old commands cannot be auto-completed by tab key or shown by “?”). The old command must be fully entered manually to be used.

A warning message will be shown when a **commit** is done using a deprecated command.

Here is an example:

On PicOS 2.4, the command of “set interface management-ethernet” was deprecated and replaced by “set system management-ethernet.”
This means that both of these commands work on PicOS 2.4, and the “interface management-ethernet” will be removed in a future release (9 months after PicOS 2.4 is published).

When using "set interface management-ethernet” in CLI, user will get the following information:

Configure node "interface management-ethernet" has been deprecated in version 2.4, please use "system management-ethernet" instead.

> ⚠ Note: The prompted information will not disappear until you remove the deprecated command.

When upgrading an image from an old version to a new one with configuration save, there will be some configuration nodes that are marked as deprecated in the new version, and user will get some notice information when committing in CLI.

For example, the following example reflects what may have happened during an upgrade from 2.3 to 2.4 with configuration saved, after upgrading and removing VLAN:

```
admin@XorPlus# delete vlans vlan-id 111
Deleting:
111 {
}
OK
admin@XorPlus# commit
Commit OK.
Configure node "interface management-ethernet" has been deprecated in version 2.4, please use "system management-et
Configure node "system syslog host" has been deprecated in version 2.4, please use "system syslog server-ip" instea
Configure node "system syslog port-number" has been deprecated in version 2.4, please use "system syslog server-ip"
Configure node "system syslog port-protocol" has been deprecated in version 2.4, please use "system syslog server-i
Save done.
admin@XorPlus#
```

> ⚠ When upgrading image from an old version to a new one, with a configuration that contains deprecated nodes, the upgrade will fail. Remove the deprecated nodes on the configuration tree. Then, install upgrade again.

Set CLI

We support setting some values for CLI.

```
admin@XorPlus> set cli ?
Possible completions:
idle-timeout Set maximum idle time before login session ends
screen-length Set terminal screen length
terminal Set terminal type
admin@XorPlus> set cli screen-length ?
Possible completions:
<length> Number of lines of text that the terminal screen displays (0..10,000).
admin@XorPlus> set cli ?
Possible completions:
idle-timeout Set maximum idle time before login session ends
screen-length Set terminal screen length
terminal Set terminal type
admin@XorPlus> set cli idle-timeout 0
admin@XorPlus> set cli screen-length ?
Possible completions:
<length> Number of lines of text that the terminal screen displays (0..10,000).
admin@XorPlus> set cli screen-length 0
admin@XorPlus>
admin@XorPlus> set cli terminal ?
Possible completions:
ansi ANSI-compatible terminal
linux Linux-compatible terminal
vt100 VT100-compatible terminal
xterm Xterm window terminal
admin@XorPlus> set cli terminal
```

CLI Configuration

This chapter describes the different ways to configure PicOS and demonstrates the CLI configuration.

There are 2 CLI's used to configure PicOS:

- The Linux CLI
- The PicOS CLI

The Linux CLI is a standard debian based bash shell.

A good Bash tutorial can be found at this address:
http://www.tldp.org/LDP/Bash-Beginners-Guide/html/

PicOS added some commands to the standard Bash shell:

Version - This is to provide the PicOS version running on the switch

```
admin@XorPlus:~$ version
Copyright (C) 2009-2022 Pica8, Inc.
===================================
Hardware Model                : N3248PXE-ON
Linux System Version/Revision : 2.5/17907
Linux System Released Date    : 10/14/2021
L2/L3 Version/Revision        : 2.5/17907
L2/L3 Released Date           : 10/14/2021
OVS/OF Version/Revision       : 2.5/17907
OVS/OF Released Date          : 10/14/2021
```

cli - command to move to the PicOS command or launch PicOS CLI commands from the Linux shell.

```
admin@XorPlus$cli
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on XorPlus
admin@XorPlus>
```

In the above example, the cli command is used to move to the PicOS CLI.

```
admin@XorPlus$cli -c "show version"
Synchronizing configuration...OK.
Welcome to PicOS L2/L3 on XorPlus
admin@XorPlus>
Execute command: show version
.
Copyright (C) 2009-2022 Pica8, Inc.
===================================
Hardware Model                : N3248PXE-ON
Linux System Version/Revision : 2.5/17907
Linux System Released Date    : 10/14/2021
L2/L3 Version/Revision        : 2.5/17907
L2/L3 Released Date           : 10/14/2021
OVS/OF Version/Revision       : 2.5/17907
OVS/OF Released Date          : 10/14/2021
```

In the command above, the cli command is used to launch commands of the PicOS CLI from the Linux shell.

Configuring Multi-window Command Configuration Display on The User Terminal

Introduction

By setting the function of multi-window command configuration on the user terminal, you can control whether or not to synchronously print the configurations of the same switch from other CLI windows to the current CLI interface.

The CLI window will not synchronously print the configurations of the same switch from other CLI windows to the current CLI interface if disables the function of multi-window command configuration on the user terminal.

Here is an example:

If you open a window, for example Window A, login a switch and set **syslog notify off**, and then the CLI configurations of this switch on any other terminal window will not be displayed to Window A synchronously. But if you set **syslog notify on** on Window A, and then CLI configurations of this switch on any other terminal window will be displayed to Window A synchronously.

NOTE :

- The function is window dependent, that is, it will take effect based on CLI windows regardless of the CLI login method (Console or SSH) or the login IP of terminal or the login users.
- When the window is restarted, the configuration of multi-window command configuration display on the user terminal function will go to the default value.

Configuring Multi-window Command Configuration Display on The User Terminal

Procedure

- From the "**>**" prompt, use the following command to disable or enable the function of multi-window command configuration display on the user terminal.

  syslog notify <**on | off**>

  The default setting is **syslog notify on**.

Configuration Example

- Enable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify on
```

- Disable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify off
```

Configuration Saving Guide

Introduction

> **Warning:**
>
> On FS S5810 Series, S3410 Series and S5860 Series switches, you have to do configuration saving described below. This specific save command is requested by hardware vendor due to the Flash limitation on numbers of write/erase cycles.

FS S5810 Series, S3410 Series and S5860 Series switches use the OverlayFS file system with which the running configuration files on the switch will not be saved from the RAM to the flash automatically. Therefore, when the power is turned off, the configuration is lost.

You need to manually issue the configuration saving command to save the configuration file from the RAM to the flash every time when you perform the following operations.

- Modify the password after PICOS installation(not including the first modification)
- Perform picos_boot
- Set L2 / L3 CLI commands (for the L2 / L3 CLI configuration, you need to issue the **commit** command before saving the configuration to flash)
- Set OVS commands
- Set Crossflow commands

You can use either one of the following two methods to save your configuration, using the **save_config** command or the **copy running-config startup-config** command:

- Method 1: Under Linux bash, issue the following command manually (When setting OVS commands, you can only use this command to save the configuration file):

```
admin@Xorplus$ sudo save_config
```

- Method 2: In the L2/L3 CLI operating mode, issue the following command manually:

```
admin@Xorplus> copy running-config startup-config
```

System Administration

- Configuring Management Interface
  - In-Band Management Interface
  - Out-of-band Management Interface
- Configuring User Account and Login Banner
- Configuring SSH and Telnet Parameters
- Configuring the Log-in ACL
- AAA Configuration Guide
  - Introduction
  - Configuration Notes of AAA
  - TACACS+ Configuration
  - RADIUS Configuration
  - Local Authentication Configuration
  - Sample configuration file on the AAA server
- NAC Configuration Guide
  - Configuration Notes of NAC
  - Configuring NAC
  - Configuration Example of NAC
  - Typical Configuration of NAC
  - References
  - Principle of NAC
- Configuring NTP and the Time Zone Parameter
- Configuring PTP
- Configuring the linux-config-unreliable
- Configuring IPFIX
- Configuring sFlow
- Configuring the Syslog Log Level
- Configuring the Syslog Disk and Syslog Server
- Displaying System Information
- IPv6 Management Support
- Configuring NETCONF
- SNMP Configuration
  - Configuring SNMPv2
  - Configuring SNMPv3
  - Configuring SNMP ACL
  - Pica8 Private MIB
  - Pica8 Public MIB
  - SNMP Monitoring and Integration with Zabbix
- PoE Configuration Guide
  - Configuring PoE
  - PoE over LLDP Power Negotiation
  - UPoE
  - Configuring Perpetual PoE
- Configuring USB Disable
- Configuring CPU Usage Alarm Threshold
- Configuring MAC Usage Alarm Threshold
- Mirror Configuration
  - Introduction of Mirroring
  - Configuration Notes of Mirroring
  - Configuring Mirror
  - Example for Configuring Local Port Mirroring
  - Example for Configuring ERSPAN
  - Example for Configuring ACL-based ERSPAN
- Configuring gNMI-gRPC Based Telemetry Technology
- Remote Network Monitoring (RMON)
  - Overview of RMON
  - Configuring RMON
  - Example for Configuring RMON
- RESTCONF Configuration
  - Introduction of RESTCONF
  - RESTCONF Operation Methods
  - Configuring RESTCONF
- EFM OAM Configuration
  - Introduction of EFM OAM
  - Configuring EFM OAM
- Configure Telnet to Access to the Remote Device

Configuring Management Interface

- In-Band Management Interface
- Out-of-band Management Interface

In-Band Management Interface

- Configuring In-Band Management Interface
- Default Settings for In-Band Management Interface on S3410 Series Switches

Configuring In-Band Management Interface

NOTE:

Only the L3 VLAN interfaces/loopback interface/routed interface/sub-interface in the default VRF can be set as the in-band management ports. If an L3 interface has been set as an in-band management port, it can only stay in the default VRF, but not any user-defined VRFs.

By default, the user cannot remotely log in and manage the switch through an L3 VLAN interface, a loopback interface, a routed interface or a sub-interface. You need to enable the in-band management function by using the following commands to perform the SSH, TELNET, SNMP and HTTP services through the L3 interface in the default VRF:

set system inband vlan-interface <*vlan-interface-name*>

set system inband loopback <*ip-address*>

set system inband routed-interface <*routed-interface-name*>

Example

- The following commands set the L3 VLAN interface VLAN400 in the default VRF as the in-band management port.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 40
0
admin@XorPlus# set vlans vlan-id 400 l3-interface vlan400
admin@XorPlus# set l3-interface vlan-interface vlan400 address 192.168.1.1 prefix-length 24
admin@Xorplus# set system inband vlan-interface vlan400
admin@Xorplus# commit
```

- The following commands set the loopback interface IP in the default VRF as the in-band management IP.

```
admin@Xorplus# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@Xorplus# set system inband loopback 1.1.1.1
admin@Xorplus# commit
```

- The following commands set the routed interface rif-ge3 in the default VRF as the in-band management port.

```
admin@XorPlus# set vlans reserved-vlan 80-90
admin@XorPlus# set interface gigabit-ethernet te-1/1/3 routed-interface enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/3 routed-interface name rif-te3
admin@XorPlus# set l3-interface routed-interface rif-te3
admin@XorPlus# set l3-interface routed-interface rif-te3 address 172.168.10.10 prefix-length 24
admin@Xorplus# set system inband routed-interface rif-te3
admin@Xorplus# commit
```

In-band management provides a method of access to the switch even if the Ethernet0/1 interface is down.

Default Settings for In-Band Management Interface on S3410 Series Switches

Overview

NOTEs:

- Currently, only S3410 Series switches support this feature.
- The VLAN interface *inband-mgmt* cannot be deleted.
- By default, all ethernet ports are enabled. If you run command **set interface gigabit-ethernet disable true** to disable ports, please make sure that at least one port in VLAN 1 is always enabled.

By default, the in-band management interface, VLAN interface *inband-mgmt*, is configured with the factory default IP address 192.168.1.1/24 based on VLAN 1. In this way, when you cannot obtain valid IP address or with no eth0 management interface to access the switch, a built-in IP address of the in-band management interface is applied, which makes sure that the switch can be always accessed by the direct connection PC.

The switch can obtain an IP address through three ways, prioritized as follows: **static IP address > dynamic IP address assigned by DHCP > factory default IP address**. When the switch can obtain an IP address through higher-priority way, the others will be disregarded. The detailed matching process is as follows:

1. By default, the DHCP client function is enabled. When the switch boots, it attempts to obtain IP address through DHCP assignment before loading configuration files, if successful, it uses this IP address; if fails to obtain in 1 minutes, it uses the factory default IP address.
2. When the switch loads configuration files with a static IP address, or when you specify an IP address for the in-band management interface *inband-mgmt*, it uses the configured IP address. For details on modifying the IP address of the in-band management interface *inband-mgmt*, refer to the next section.

NOTEs:

- When the switch uses the factory default IP address, it will continue to attempt to obtain an IP address from the DHCP server. If successful, it will use the assigned IP address instead of the default IP address.
- When the switch uses the IP address assigned by DHCP server, if the IP address lease is out of date and the switch cannot communicate with DHCP server, the IP address will be covered with 0.0.0.0 and the switch will execute the matching process again to obtain the IP address.

Modifying the IP Address

NOTE:

Please be cautious to perform this operation. If the IP address of in-band management interface is modified, the user login session will be interrupted, and you need to log in again with the new IP address.

To modify the default IP address of interface *inband-mgmt*, take the following steps:

Step 1 Disable the DHCP function.

set l3-interface vlan-interface inband-mgmt dhcp false

Step 2 Specify the IP address for interface *inband-mgmt*.

set l3-interface vlan-interface inband-mgmt address <*ipv4-address* | *ipv6-address*> **prefix-length** <*length*>

Step 3 Commit the configuration. If you configure multiple IP addresses, the latest configuration is valid.

Commit

Step 4 View the *inband-mgmt* configuration information.

run show l3-interface vlan-interface inband-mgmt

Step 5 Restore the IP address to default value 192.168.1.1.

rollback default

Out-of-band Management Interface

- Configuring Port Speed of eth0 Out-of-Band Management Interface
- Default Settings for Out-of-band Management Interface

Configuring Port Speed of eth0 Out-of-Band Management Interface

The management interface **eth0** is a special Ethernet interface that provides configuration management support for the user, that is, the user can log on to the device and perform configuration and management operations through this interface. The **eth0** management interface is not responsible for the transmission of data services.

The following command can be used to configure the port speed (in Mbit/s) of **eth0** out-of-band management interface in operational mode.

set management-ethernet-speed eth0 <**10 | 100 | 1000 | auto**>

Example

- Configure port speed of **eth0** out-of-band management interface to 100Mbit/s and show the configuration result.

```
admin@PICOS> set management-ethernet-speed eth0 100
admin@PICOS> start shell sh
admin@PICOS:~$ sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  Not reported
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: No
        Advertised FEC modes: Not reported
        Speed: 100Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 2
        Transceiver: internal
        Auto-negotiation: off
        MDI-X: Unknown
```

Default Settings for Out-of-band Management Interface

By default, the out-of-band management interface *eth0* is configured with the factory default IP address 192.168.1.1/24. In this way, when you cannot obtain valid IP address to access the switch, a built-in IP address is applied, which makes sure that the switch can be always accessed by the direct connection PC.

The switch can obtain an IP address through three ways, prioritized as follows: **static IP address > dynamic IP address assigned by DHCP > factory default IP address**. When the switch can obtain an IP address through higher-priority way, the others will be disregarded. The detailed matching process is as follows:

1. Initially, the switch uses the factory default IP address before PicOS boots up. The DHCP client function is enabled by default, and the switch attempts to obtain IP address through DHCP assignment when PicOS boots up, if successful, it uses this IP address; if fails to obtain in 1 minutes, it uses the factory default IP address.
2. When the switch loads configuration files with a static IP address, or when you specify an IP address for the interface *eth0*, it uses the configured IP address. For details on modifying the IP address of the out-of-band management interface *eth0*, refer to the next section.

Modifying the IP Address

To modify the default IP address of interface *eth0*, take the following steps:

Step 1 Specify the IP address for interface *eth0*. Meanwhile, the DHCP client function is disabled.
set system management-ethernet eth0 ip-address IPv4 <*ipv4-address*>

Step 2 Commit the configuration. If you configure multiple IP addresses, the latest configuration is valid.
Commit

Step 3 View the configuration information of interface *eth0*.
run show system management-ethernet

To delete the specified IP address of interface *eth0*, use the command **delete system management-ethernet eth0 ip-address IPv4**. Meanwhile, the DHCP client function is enabled.

Configuring User Account and Login Banner

There are two types of user accounts: **super-user** and **read-only**. The newly created user account, by default, is read-only.

> **NOTE:**
> "**net-admin**" is not allowed to use when configuring a username.

Creating a User Class and Password

```
admin@XorPlus# set system login user ychen authentication plain-text-password pica8
admin@XorPlus#set system login user ychen class super-user
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a Login Announcement after Login

```
admin@XorPlus# set system login announcement "welcome the switch-1101"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a Multi-line Login Announcement after Login

The following example configures a multi-line announcement which will be printed on the teminal after user login.

```
admin@XorPlus# set system login multiline-announcement 1 message "*********************************************"
admin@XorPlus# set system login multiline-announcement 2 message "Welcome to the system！"
admin@XorPlus# set system login multiline-announcement 3 message "*********************************************"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a Login Banner before Login

```
admin@XorPlus# set system login banner "Hello! Welcome!"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a Multi-line Login Banner before Login

The following example configures a multi-line banner which will be printed on the teminal before user login.

```
admin@Xorplus# set system login multiline-banner 1 message "********************NOTICE**********************"
admin@Xorplus# set system login multiline-banner 2 message "This is a property of Pica8."
admin@Xorplus# set system login multiline-banner 3 message "All users log-in are subject to company monitoring!"
admin@Xorplus# set system login multiline-banner 4 message "************************************************"
admin@Xorplus# commit
```

Configuring SSH and Telnet Parameters

Configuring the SSH Connection Limit

```
admin@XorPlus# set system services ssh protocol-version v2
admin@XorPlus# set system services ssh connection-limit 5
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Enabling and Disabling Inband Service

By default, SSH with inband interfaces are disabled. You can enable inband services by entering the command below.

- Set the L3 VLAN interface VLAN400 in the default VRF as the in-band management port.

```
admin@Xorplus# set system inband vlan-interface VLAN400
admin@Xorplus# commit
```

- Set the loopback interface IP in the default VRF as the in-band management IP.

```
admin@Xorplus# set system inband loopback 192.168.10.1
admin@Xorplus# commit
```

- Set the routed interface rif-ge3 in the default VRF as the in-band management port.

```
admin@Xorplus# set system inband routed-interface rif-ge3
admin@Xorplus# commit
```

Configuring the Idle Timeout for SSH User

```
admin@Xorplus# set system services ssh idle-timeout 60
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the Port Number of the SSH server

Users can use this command to configure the new port number of SSH server to prevent attackers from accessing the standard port of SSH service and ensure security. The default listening port number of the SSH server is 22.

Note that, if the modified port number is not 22, the client needs to specify port number when logging in using SSH.

```
admin@Xorplus# set system services ssh port 30
admin@Xorplus# commit
```

Enabling Telnet Service

The Pica8 switch supports functioning as a telnet server. To enable the telnet server function, users can enable the telnet service.

The following command enables telnet service on the device.

NOTEs:

- Telnet service is insecure. Do not enable a telnet server if you don't know what exactly it may mean.

- Limit to a maximum of 20 connections within 10 seconds.
- Terminate the session in 60 seconds if the connection is not successful.

```
admin@PICOS# set system services telnet disable false
admin@PICOS# commit
```

Configuring the Log-in ACL

Configure the ACL to control whether remote hosts within specified sub-networks are allowed to log in to the system. In our example, remote hosts from both sub-networks that we configured may log in.

```
admin@XorPlus# set system login-acl network 192.168.1.0/24
admin@XorPlus# set system login-acl network 192.168.100.100/32
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

AAA Configuration Guide

- Introduction
- Configuration Notes of AAA
- TACACS+ Configuration
- RADIUS Configuration
- Local Authentication Configuration
- Sample configuration file on the AAA server

Introduction

AAA (Authentication, Authorization and Accounting) is a management mechanism of network security and provides three security functions of authentication, authorization and accounting.

Authentication: Confirm the identity of remote users accessing the network to determine whether the visitor is a validated network user.

Authorization: Give different users with different permissions, restriction to services that users can use. For example, after the user successfully logs in to the server, the administrator can authorize the user to execute CLI commands.

Accounting: Record all operations of users using network services, including the type of service used, starting time, data traffic, etc. It is not only a means of billing, but also monitors network security.

PICOS supports TACACS+, RADIUS and local authentication method. TACACS+ (Terminal Access Controller Access Control System) is a security protocol that is an enhancement to the original TACACS protocol. The protocol is similar to the RADIUS protocol. It uses the client / server model to communicate with the NAS and the TACACS + server to achieve user's AAA management.

TACACS+/RADIUS Authentication and Authorization Process

This section describes the TACACS+/RADIUS authentication and authorization of PICOS 2.11.7 and the later versions.

	TACACS+/RADIUS server is reachable and TACACS+/RADIUS service is configured	TACACS+/RADIUS server is unreachable or TACACS+/RADIUS service is not configured
Console Login	Allow to login only if pass authentication form TACACS+ server.	Generate a syslog and fallback to local authentication. Allow to login if pass local authentication. After successful login, local authorization will be performed. By default, generate a syslog and do nothing else.
Network (INTERFACE/VLAN/MGMT Port/INBAND) Login	After successful login, if the TACACS+ server goes down, the user will be logged out and asked to re-log in.	User can configure to enable local authentication fallback function to fallback to local authentication and authorization in this case. For details about local authentication fallback function, see set system aaa local-auth-fallback disable.

Console Login:

- If the TACACS+/RADIUS server is reachable and the TACACS+/RADIUS service is configured, the system uses TACACS/RADIUS server for authentication. Access will be denied on failure. After successful login, if the TACACS+ server goes down, the user will be logged out and asked to re-log in.
- If the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, the system generates a syslog and uses local user/passwd file for authentication. After successful login, local authorization will be performed.

Network (INTERFACE/VLAN/MGMT Port/INBAND) Login:

- If the TACACS+/RADIUS server is reachable and the TACACS+/RADIUS service is configured, the system uses TACACS+/RADIUS server for authentication. Access will be denied on failure. After successful login, if the TACACS+ server goes down, the user will be logged out and asked to re-log in.
- If the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, by default, the system generates a syslog and does nothing else. However, user can configure local authentication fallback function to perform local authentication and authorization. For details about local authentication fallback function, see set system aaa local-auth-fallback disable.

User Level Mapping

If users login to PICOS via TACACS+/RADIUS, PICOS will not create new users in Linux platform. There is a mapping relationship between user level configured on AAA server and PICOS local user. The following table lists the mapping relationship between TACACS+ user and local user.

Howerver, note that RADIUS user is mapped to admin when login to PICOS.

Table 1. User level mapping between TACACS+ user level and PICOS local user

User Level on TACACS+ Server	User Account	Permission Class	Descriptions
15	admin	Super-user	Users of this level can configure network services, such as routing and commands of all network layers, and can control basic system operations and user management.

1-14	operator	Read-only	Users of this level can access to **configuration** mode to view the current configuration with limited access. A network operator cannot modify any configuration setting on a switch.
0	guest	Guest	Users of this level can do nothing but show the version and exit.

Configuration Notes of AAA

When configuring AAA on a device, pay attention to the following points:

- TACACS+ and RADIUS cannot be used at the same time. If both TACACS+ and RADIUS are enabled, then TACACS+ is valid but RADIUS is invalid.
- Users authenticate with the AAA server to gain access to the NAS server when AAA function is enabled. Make sure that the communication between the NAS server and AAA server works well.
- If the same accounts of admin/root/operator are used in conjunction with TACACS, TACACS authorization will be ignored and the local account policy will take precedence.
- For redundancy management of AAA server, multiple remote AAA servers can be configured at the same time. Only one server can be used at the same time. However, there are a few differences between TACACS + and RADIUS validation.
  - If user validation on one TACACS+ server fails, it will switch to the other reachable TACACS+ servers for validation automatically.
  - Only one RADIUS server with the smallest IP address will be used for user validation, if user validation on one RADIUS server fails, it will not use the other reachable RADIUS servers for validation.
- When the AAA server is unreachable, users who have logged in successfully will quit CLI interface and fallback to Linux shell when they execute the CLI command that needs to be authorized.
- If the value of the shared key is different from that of the TACACS+/RADIUS server,
  - For RADIUS, it is considered that the RADIUS server is unreachable.
  - For TACACS+, it is considered that the TACACS+ server is reachable but the authentication failed.
- When resetting any AAA radius / TACACS + configuration, the new setting takes effect only for the subsequent users who log in to the CLI. For example, change the IP of the current TACACS+ server.

  Note that：For online users who have already passed AAA Authentication and successfully logged in are not affected by the resetting configurations. If the user logs out and then logs in again, the system will use the new configurations for AAA Authentication.

TACACS+ Configuration

TACACS + uses TCP reliable transmission and data encryption transmission, it is a more secure AAA feature.

PicOS supports a maximum of eight TACACS+ servers. When multiple TACACS+ servers are configured, only one will be used, the IP addresses are used in alphabetical order.

For example, the following TACACS+ servers are configured.

```
set system aaa tacacs-plus server-ip 146.13.191.77
set system aaa tacacs-plus server-ip 146.13.191.78
set system aaa tacacs-plus server-ip 1.1.1.1
set system aaa tacacs-plus server-ip 2.2.2.2
set system aaa tacacs-plus server-ip 3.3.3.3
```

The servers will be used in below order.

1. 1.1.1.1
2. 146.13.191.77
3. 146.13.191.78
4. 2.2.2.2
5. 3.3.3.3

Configuring TACACS+

Procedure

Step1 Enable TACACS+ function.

set system aaa tacacs-plus disable <true | false>

Step2 Configure TACACS+ shared key.

set system aaa tacacs-plus key *<string>*

The value of TACACS+ shared key should be the same with that on the TACACS+ servers. The shared key should have a same value on different TACACS+ servers.

Step3 Configure IP address of TACACS+ server.

set system aaa tacacs-plus server-ip *<ipv4_address>*

Step4 (Optional) Configure the port number of TACACS+ server.

set system aaa tacacs-plus port-number *<integer>*

By default, the port number of TACACS+ server is 49. The value of port number should be the same with that on the TACACS+ servers.

Step5 Configure the source interface.

set system aaa tacacs-plus source-interface *<interface-name>*

Step6 (Optional) Configure TACACS+ connection timeout.

set system aaa tacacs-plus timeout *<integer>*

By default, the value of TACACS+ connection timeout is 5 seconds.

Step7 (Optional) Configure TACACS+ authentication type.

set system aaa tacacs-plus auth-type <ascii | chap | pap>

By default, the TACACS+ authentication type is ascii.

Step8 (Optional) Enable TACACS+ authorization. By default, TACACS+ authorization is enabled.

set system aaa tacacs-plus authorization <true | false>

Step9 (Optional) Enable TACACS+ accounting. By default, TACACS+ accounting is enabled.

set system aaa tacacs-plus accounting <true | false>

Step10 Commit the configurations.

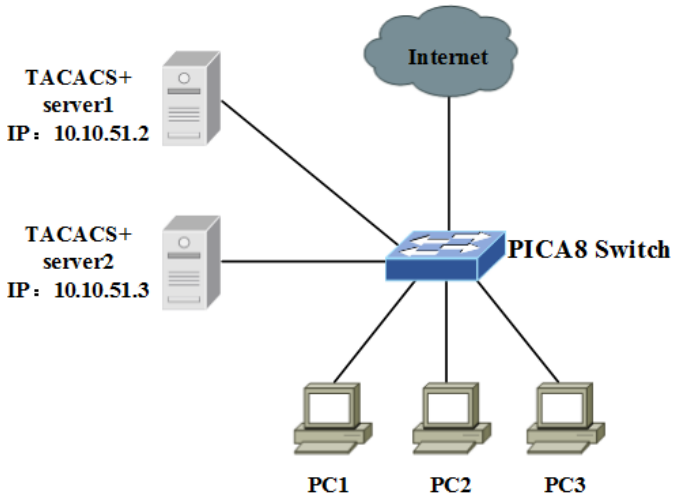
commit

TACACS+ Configuration Example

Networking Requirements

As shown in Figure 1, PC1, PC2, and PC3 connect to the internet through the PICA8 Switch. Configure TACACS+ function on PICA8 Switch to accomplish authentication, authorization, and accounting of PC1, PC2, and PC3 through TACACS + server1 and TACACS + server2. Suppose PICA8 Switch connects to the TACACS + servers through management interface eth0.

Figure 1. TACACS+ Networking Topology



Procedure

Step1 Enable TACACS+ function.

```
admin@XorPlus# set system aaa tacacs-plus disable false
```

Step2 Configure shared key of the TACACS+ servers.

```
admin@XorPlus# set system aaa tacacs-plus key pica8pica8
```

Step3 Configure TACACS+ server IP.

```
admin@XorPlus# set system aaa tacacs-plus server-ip 10.10.51.2
admin@XorPlus# set system aaa tacacs-plus server-ip 10.10.51.3
```

Step4 (Optional) Configure the port number of TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus port-number 50
```

Step5 Configure the source interface.

```
admin@XorPlus# set system aaa tacacs-plus source-interface eth0
```

Step6 (Optional) Configure TACACS+ connection timeout.

```
admin@XorPlus# set system aaa tacacs-plus timeout 30
```

Step7 (Optional) Configure TACACS+ authentication type.

```
admin@XorPlus# set system aaa tacacs-plus auth-type chap
```

Step8 Commit the configurations.

```
admin@XorPlus# commit
```

Check the Configuration

- You can use the **show system aaa tacacs-plus** command to view the configuration information of TACACS+.

```
admin@XorPlus# show system aaa tacacs-plus
disable: false
server-ip 10.10.51.2
server-ip 10.10.51.3
key: "QT09cGljYThwaWNhOA==Y0ds"
source-interface: "eth0"
```

RADIUS Configuration

As the RADIUS protocol is simple and scalable, it is the most widely used AAA protocol.

Configuring RADIUS

Procedure

Step1 Enable RADIUS authentication and authorization.

set system aaa radius authorization disable <true | false>

Step2 Configure IP address of RADIUS authentication and authorization server.

set system aaa radius authorization server-ip <*ipv4_address*>

Step3 Configure port number of RADIUS authentication and authorization server.

set system aaa radius authorization server-ip <*ipv4_address*> **port** <*integer*>

By default, the port number of RADIUS authentication and authorization server is 1812. The value of port number should be the same with that on the RADIUS servers.

Step4 Configure RADIUS authentication and authorization shared key.

set system aaa radius authorization server-ip <*ipv4_address*> **shared-key** <*string*>

The value of RADIUS authentication and authorization shared key should be the same with that on the RADIUS server.

Step5 Configure the source interface.

set system aaa radius source-interface <*interface-name*>

Step6 Configure RADIUS authentication and authorization connection timeout.

set system aaa radius authorization server-ip <*ipv4_address*> **timeout** <*integer*>

By default, the value of RADIUS authentication and authorization connection timeout is 5 seconds.

Step7 Enable RADIUS accounting function.

set system aaa radius accounting disable <true | false>

Step8 Configure RADIUS accounting server IP.

set system aaa radius accounting server-ip <*ipv4_address*>

Step9 Configure port number of RADIUS accounting server.

set system aaa radius accounting server-ip <*ipv4_address*> **port** <*integer*>

By default, the port number of RADIUS accounting server is 1813. The value of port number should be the same with that on the RADIUS servers.

Step10 Configure RADIUS accounting shared key.

set system aaa radius accounting server-ip <*ipv4_address*> **shared-key** <*string*>

Step11 Configure RADIUS accounting connection timeout.

set system aaa radius accounting server-ip <*ipv4_address*> **timeout** <*integer*>

Step12 Commit the configurations.

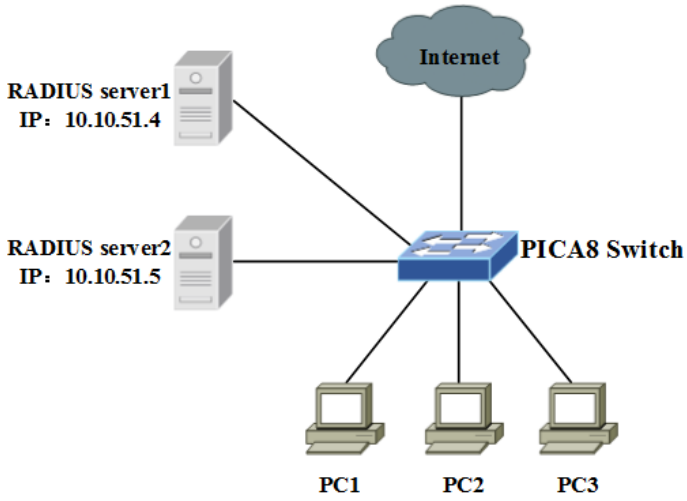
commit

Configuration Example

Networking Requirements

As shown in Figure 1, PC1, PC2, and PC3 connect to the internet through the PICA8 Switch. Configure RADIUS function on PICA8 Switch to accomplish authentication, authorization, and accounting of PC1, PC2, and PC3 through RADIUS server1 and RADIUS server2.

Figure 1. RADIUS Networking Topology



Procedure

Step1 Enable RADIUS authentication and authorization.

```
admin@XorPlus# set system aaa radius authorization disable false
```

Step2 Configure IP address of RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.4
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.5
```

Step3 Configure port number of RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.4 port 1800
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.5 port 1800
```

By default, the port number of RADIUS authentication and authorization server is 1812.

Step4 Configure RADIUS authentication and authorization shared key.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.4 shared-key pica8
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.5 shared-key pica8
```

The value of RADIUS authentication and authorization shared key should be the same with that on the RADIUS server.

Step5 Configure the source interface.

```
admin@XorPlus# set system aaa radius source-interface eth0
```

Step6 Configure RADIUS authentication and authorization connection timeout.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.4 timeout 30
admin@XorPlus# set system aaa radius authorization server-ip 10.10.51.5 timeout 30
```

By default, the value of RADIUS connection timeout is 5 seconds.

Step7 Enable RADIUS accounting.

```
admin@XorPlus# set system aaa radius accounting disable false
```

Step8 Configure IP address of RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.4
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.5
```

Step9 Configure port number of RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.4 port 1801
```

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.5 port 1801
```

By default, the port number of RADIUS accounting server is 1813.

Step10 Configure RADIUS accounting shared key.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.4 shared-key pica8
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.5 shared-key pica8
```

Step11 Configure RADIUS accounting connection timeout.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.4 timeout 30
admin@XorPlus# set system aaa radius accounting server-ip 10.10.51.5 timeout 30
```

Step12 Commit the configurations.

```
admin@XorPlus# commit
```

Check the Configuration

- You can use the **show system aaa radius** command to view the configuration information of RADIUS.

```
admin@XorPlus# show system aaa radius
radius {
        authorization {
            disable: false
            server-ip 10.10.51.4 {
                 timeout: 30
                port: 1800
            }
            server-ip 10.10.51.5 {
                timeout: 30
                port: 1800
            }
        }
        accounting {
            disable: false
            server-ip 10.10.51.4{
                timeout: 30
                port: 1801
            }
            server-ip 10.10.51.5 {
                timeout: 30
                port: 1801
            }
        }
```

Local Authentication Configuration

This chapter describes the configuration of local authentication.

Configuring Local Authentication

> **NOTE:**
> The local authentication and authorization is enabled by default if remote authentication and authorization is not deployed, the access users are authenticated and authorized based on the local user information.

Step1 Enable local authentication.

set system aaa local disable <true | false>

Step2 Commit the configuration.

commit

Configuring a Local User

When local authentication is configured, configure authentication and authorization information on the device, including the user name, password, and user level.

Step1 Configure a local user account.

set system login user <*username*> **authentication plain-text-password** <*password*>

Step2 Configure user authorization.

set system login user <*username*> **class** <**read-only** | **super-user**>

By default, the newly created user is read-only.

Step3 Commit the configuration.

commit

Example for Configuring Local Authentication

Step1 Enable local authentication.

```
admin@XorPlus# set system aaa local disable false
```

Step2 Commit the configuration.

```
admin@XorPlus# commit
```

Example for Configuring a Local User

Step1 Configure a local user account **manager**.

```
admin@XorPlus# set system login user manager authentication plain-text-password 123456
```

Step2 Configure the user as super-user for user account **manager**.

```
admin@XorPlus# set system login user manager class super-user
```

Step3 Commit the configuration.

```
admin@XorPlus# commit
```

Sample configuration file on the AAA server

Here is a sample configuration file on the AAA server.

```
key = pica8

Accounting File
accounting file = /var/tmp/acctfile
default authentication = file /etc/passwd
user = admin {
member = admins
}
group = admins {
global = cleartext "password"
service = exec {
default attribute = permit
}
}
user = operator {
global = cleartext "operator"
service = exec {
default attribute = permit
}
}
user = ychen {
global = cleartext "ychen"
member = admins
service = exec {
default attribute = permit
}
}
Add "/usr/share/freeradius/dictionary.pica8" to radius server before the configuration.

Radius server configuration:
operator Cleartext-Password := "testing"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 172.16.3.33,
Framed-IP-Netmask = 255.255.255.0,
Framed-Routing = Broadcast-Listen,
Framed-Filter-Id = "std.ppp",
Framed-MTU = 1500,
Framed-Compression = Van-Jacobsen-TCP-IP,
Class = "read-only"
ychen Cleartext-Password := "testing"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 172.16.3.33,
Framed-IP-Netmask = 255.255.255.0,
Framed-Routing = Broadcast-Listen,
Framed-Filter-Id = "std.ppp",
Framed-MTU = 1500,
Framed-Compression = Van-Jacobsen-TCP-IP,
Class = "super-user"
```

Follow the configuration above, the admin or operator can access the switch via SSH.
Any valid CLI commands executed by the admin or operator will be recorded to the specified accounting file. In our example above, the accounting file is/var/tmp/acctfile.

NAC Configuration Guide

- Configuration Notes of NAC
- Configuring NAC
- Configuration Example of NAC
  - Example for Configuring 802.1X Authentication
  - Example for Configuring MAB Authentication
  - Example for Configuring CWA Authentication
  - Example for Configuring Multiple Authentication Modes
- Typical Configuration of NAC
  - Example for Configuring NAC (PacketFence as the Authentication Server)
  - Solution Documents Download
- References
- Principle of NAC

Configuration Notes of NAC

When configuring NAC on a device, pay attention to the following points:

- 802.1X client authentication software is required on the supplicant when you use the 802.1X authentication to control the network access of the supplicant. If you only use MAB authentication to control network access of the clients, the 802.1X client software is not required.
- The MAB authentication is performed each time when the port link goes down and then up.
- 802.1X authentication is used on the port connected to the host user. It is not supported for the port connected to the AAA server.
- It is strongly recommended not to use both voice VLAN and dynamic VLAN on the port enabled with NAC function.
- The link type for the port of dynamic VLAN should be trunk port.
- 802.1X authentication only supports RADIUS protocol between the authenticator and the authentication server. It does not support TACACS/TACACS+ authentication.
- A maximum of eight NAC authenticated users are supported on each port.
- 802.1X authentication and MAB authentication cannot be configured on a LAG port or a physical port that belongs to a LAG. When we need to configure these functions on the physical port that belongs to a LAG, we must first remove the physical port from the LAG port before configuration.
- The recommended AAA servers are ClearPass, ISE and PacketFence.
- The link type of the port used for NAC function should be trunk port.
- The static firewall filter rule (set by the commands **set firewall filter** *XX*) cannot be applied to the port used for NAC function. Similarly, if a static firewall filter rule is applied to a port, then the port cannot employ NAC.
- The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, you need to enable MAB authentication on the switch first.
- In CLI configuration, you need to enable MAB authentication before enable CWA authentication.
- The CWA authentication process will be implemented after the MAB authentication fails.
- Up to 20 AAA servers can be configured (using command **set protocols dot1x aaa radius authentication server-ip** <ipv4-address> [**shared-key** <*key-string*>]); only one Web authentication server can be configured (using command **set protocols dot1x aaa web server-ip** <*ipv4-address*> **port** <*port-number*>).
- For the NAC authentication, if dynamic VLAN is not provided by the AAA server, the native VLAN will be used instead.
- The static MACs also need to be authenticated if the port is enabled with NAC.
- Rapid PVST+ blocks traffic from the dynamic VLAN delivered from the RADIUS authentication server.

Configuring NAC

Prerequisite

You need to complete the NAC configuration on both AAA server and PICA8 switch when employ NAC function. The following section describes how configure NAC on PICA8 switch. For details about how to configure NAC on AAA server, please refer to the following documents in Typical Configuration of NAC:

- Configuring Dynamic and Downloadable ACL for ClearPass
- Configuring Dynamic and Downloadable ACL on Cisco ISE
- Configuring Pica8 Switches with ClearPass Guest Central Web Authentication
- Integrating Pica8 Switches with Cisco ISE

Procedure

Step1 Configure VLAN.

a) Create a VLAN.

set vlans vlan-id <*vlan-id*>

b) Configure the interface to VLAN.

set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

c) Configure the IP address of the VLAN.

set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

d) Associate a Layer 3 interface with a VLAN.

set vlans vlan-id <vlan-id> **l3-interface** <interface-name>

Step2 Configure IP address for RADIUS authentication server and the shared key.

set protocols dot1x aaa radius authentication server-ip <*ip-address*> [**shared-key** <*key-string*>]

Step3 (Optional) Configure the UDP port for RADIUS authentication server and accounting server.

set protocols dot1x aaa radius authentication server-ip <*ip-address*> **auth-port** <*port-number*>

set protocols dot1x aaa radius authentication server-ip <*ip-address*> **acct-port** <*port-number*>

Step4 Configure the DNS serve IP address. This step is required for Web authentication.

set system dns-server-ip <*dns-server-ip*>

> **NOTEs:**
> Make sure to configure the mapping of the domain name of the redirect URL to the IP address on the DNS server.

Step5 Configure the NAS IP address to the L3 interface IP which is connected to the AAA server.

set protocols dot1x aaa radius nas-ip <*ip-address*>

This command is used to set the nas-ip field in RADIUS access-request message. It can be the IP address of a VLAN interface, eth0, routed interface or sub-interface.

Step6 Configure the authentication mode.

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x**

set protocols dot1x interface <*interface-name*> **auth-mode mac-radius**

set protocols dot1x interface <*interface-name*> **auth-mode web**

Step7 Configure block VLAN. This step is required for Web authentication.

a) Configure block VLAN ID.

set protocols dot1x block-vlan-id <*block-vlan-id*>

b) Configure the interface to VLAN.

set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

c) Configure the IP address of block VLAN interface.

set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

d) Associate a Layer 3 interface with block VLAN.

set vlans vlan-id <block-vlan-id> **l3-interface** <interface-name>

Step8 Configure a RADIUS dynamic authorization client from which the switch accepts Change of Authorization (CoA) messages. This step is required for CoA and Web authentication.

set protocols dot1x aaa radius dynamic-author client <*client-ip*> **shared-key** <*key-string*>

Step9 (Optional) Configure the UDP port of the RADIUS dynamic authorization server of CoA function. This is the UDP port on the switch side.

set protocols dot1x aaa radius dynamic-author client <*client-ip*> **port** <*port-number*>

Step10 Configure host mode for NAC authentication interface.

set protocols dot1x interface <*interface-name*> **host-mode** <**single** | **multiple**>

Step11 Configure dynamic ACL on the switch.

a) Configure the filter conditions.

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from** <*filter-condition*>

b) Configure the filter action.

set protocols dot1x filter <*filter-name*> **sequence** <*number*> **then action** <**discard** | **forward**>

> **NOTE:**
>
> The filter name configured in the Filter-Id must be the same as the filter name of the dynamic ACL configured on the switch.

Step12 (Optional) Configure a server fail VLAN on the switch.

set protocols dot1x server-fail-vlan-id <*vlan-id*>

Step13 (Optional) Enable fallback to WEB function.

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x fallback-to-web disable** <**true** |**false**>

Step14 (Optional) Enable open authentication function on a specified interface.

set protocols dot1x interface <*interface-name*> **authentication-open disable <true | false>**

Step15 (Optional) You can use either one of the following two commands to configure the maximum number of NAC sessions that are allowed to be established on the port enabled for NAC.

By default, there is no limit on the number of NAC sessions.

set protocols dot1x interface <*interface-name*> **max-sessions** <*max-sessions-number*>

set protocols dot1x max-sessions-per-port <*max-sessions-number*>

Step16 Commit the configuration.

commit

Configuration Example of NAC

- Example for Configuring 802.1X Authentication
- Example for Configuring MAB Authentication
- Example for Configuring CWA Authentication
- Example for Configuring Multiple Authentication Modes

Example for Configuring 802.1X Authentication

Networking Requirements

As shown in **Figure 1**, a large number of user terminals in a company access the Internet through ge-1/1/1 of the PICA8 Switch (as the access device). To ensure network access security, the administrator employs 802.1X authentication on the Switch and AAA server, to control the network access rights of the user terminals. The Switch allows the user terminals to access resources on the Internet only when the authentication is successfully passed.

Prerequisite

Ensure that PICA8 Switch is properly connected to the AAA server. In this example, the switch uses the management port Eth0 to connect to the AAA server.

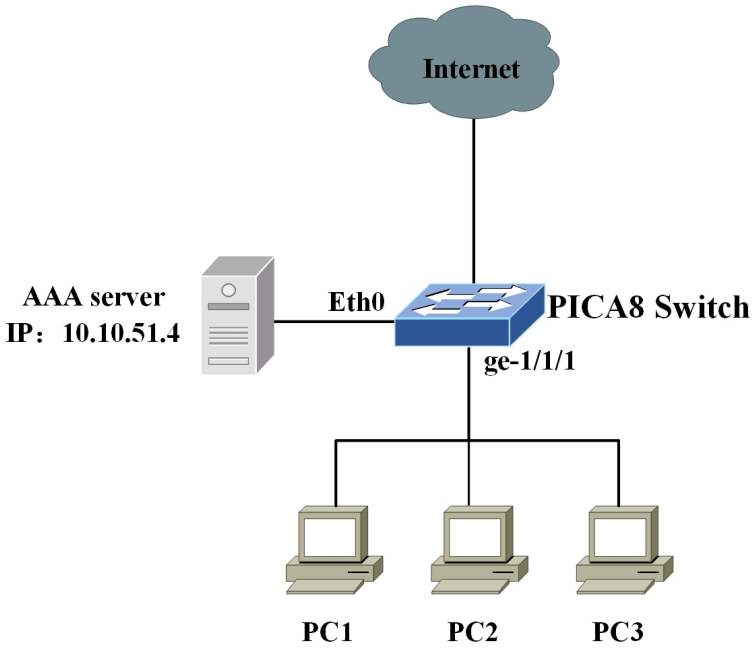
Configuration on the AAA Server

- Configure the Eth0 IP address of the switch to establish a connection to the switch.
- Configure the username and password on the AAA server.
- Configure the shared key.
- Configure other RADIUS attributes for 802.1X authentication.

Configuration on the Switch

- Use Eth0 management port connects to the AAA server.
- Configure the 802.1X authentication server IP and shared key on the Switch.
- Enable 802.1X authentication on the Switch.
- Configure the host mode to multiple on interface ge-1/1/1.

Figure 1. Networking Diagram for Configuring 802.1X Authentication



Procedure

Step1 Configure the access port to trunk mode and enable 802.1X authentication mode.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x
```

Step2 Configure IP address of AAA server and the shared key.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 10.10.51.4 shared-key pica8
```

Step3 Configure the NAS IP address to the L3 VLAN interface IP which is connected to the RADIUS server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 10.10.51.100
```

This command is used to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step4 Configure the host mode for NAC authentication interface.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 host-mode multiple
```

Step5 Commit the configuration.

```
admin@XorPlus# commit
```

Step6 Verify the configuration.

a) Run the **run show dot1x interface** to check the 802.1X authentication configurations. The command output (**802.1x = enable**) shows that the 802.1X authentication has been enabled on the interface ge-1/1/1 and MAC address ae:11:01:39:1a:00 is successfully authenticated.

```
admin@Xorplus# run show dot1x interface
Interface 802.1x  MAC-RADIUS  WEB     HOST-MODE    Session-Timeout  CLIENT-MAC       CLIENT-STATUS
-------------------------------------------------------------------------------------------------
ge-1/1/1  enable  disable     disable  multiple(3)   0              00:11:22:33:44:55  authorized
                                                                    33:12:a1:49:1b:0c authorized
                                                                    b3:55:c1:d7:2f:22 authorized
```

b) The user starts the 802.1X client software on the terminal, enters the username and password, and starts authentication.

c) If the user name and password are correct, there will be an authentication success message displayed. Then users can access the network through this port.

Example for Configuring MAB Authentication

Networking Requirements

As shown in **Figure 1**, a large number of dumb terminals (Printers in this example) in a company that access the Internet through ge-1/1/1 of the PICA8 Switch (as the access device). To ensure network access security, the administrator employs MAB authentication on the Switch and AAA server, to control the network access rights of the Printers. The Switch allows the Printers to access resources on the Internet only when the MAB authentication is successfully passed.

Prerequisite

Ensure that PICA8 Switch is properly connected to the AAA server. In this example, the switch uses the management port Eth0 to connect to the AAA server.

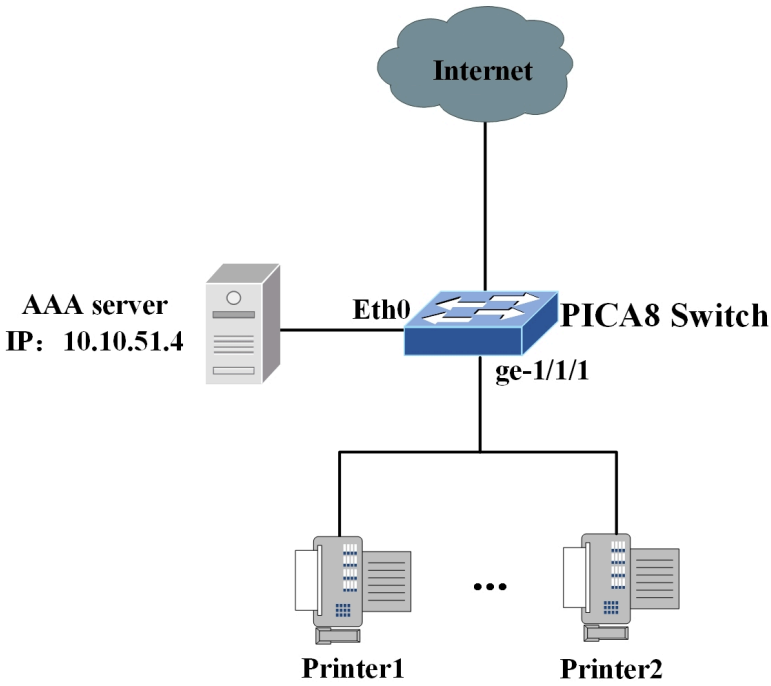
Configuration on the AAA Server

- Configure the Eth0 IP address of the switch to establish a connection to the switch.
- Configure the credentials for each printer on the AAA server.
- Configure the shared key.
- Configure other RADIUS attributes for MAB authentication.

Configuration on the Switch

- Configure the AAA server IP and shared key on the Switch.
- Enable MAB authentication on the Switch, to perform MAB authentication on terminals that cannot install the 802.1X client software.
- Configure the host mode to multiple on interface ge-1/1/1.

Figure 1. Networking Diagram for Configuring MAB Authentication



Procedure

Step1 Configure the access port to trunk mode and enable MAB authentication mode.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
```

Step2 Configure IP address of AAA server and the shared key.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 10.10.51.4 shared-key pica8
```

Step3 Configure the NAS IP address to the IP address of Eth0 interface which is connected to the AAA server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 10.10.51.100
```

This command is used to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the AAA server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step4 Configure the host mode for NAC authentication interface.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 host-mode multiple
```

Step5 Commit the configuration.

```
admin@XorPlus# commit
```

Step6 Verify the configuration.

Run the **run show dot1x interface** to check the MAB authentication configurations. The command output (**MAC-RADIUS** = **enable**) shows that the MAB authentication has been enabled on the interface ge-1/1/1 and MAC address ae:11:01:39:1a:00 is successfully authenticated.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x   MAC-RADIUS  WEB     HOST-MODE   Session-Timeout  CLIENT-MAC  CLIENT-STATUS
-------------------------------------------------------------------------------------------------
ge-1/1/1  disable   enable   disable    multiple(3)  0               ae:11:01:39:1a:00 authorized
                                                                    33:12:a1:49:1b:0c authorized
                                                                    b3:55:c1:d7:2f:22 authorized
```

Example for Configuring CWA Authentication

Networking Requirements

As shown in **Figure 1**, the terminals in the visitor area are connected to the company's internal network through the Switch. Unauthorized access to the internal network can damage the company's service system and cause leakage of key information assets. Therefore, the administrator employs the CWA on the Switch and on the Web Authentication Server of the AAA to control the users' network access rights to ensure internal network security.

Prerequisite

Ensure that PICA8 Switch is properly connected to the AAA server. In this example, the switch uses the management port Eth0 to connect to the AAA server.

Configuration on the AAA Server

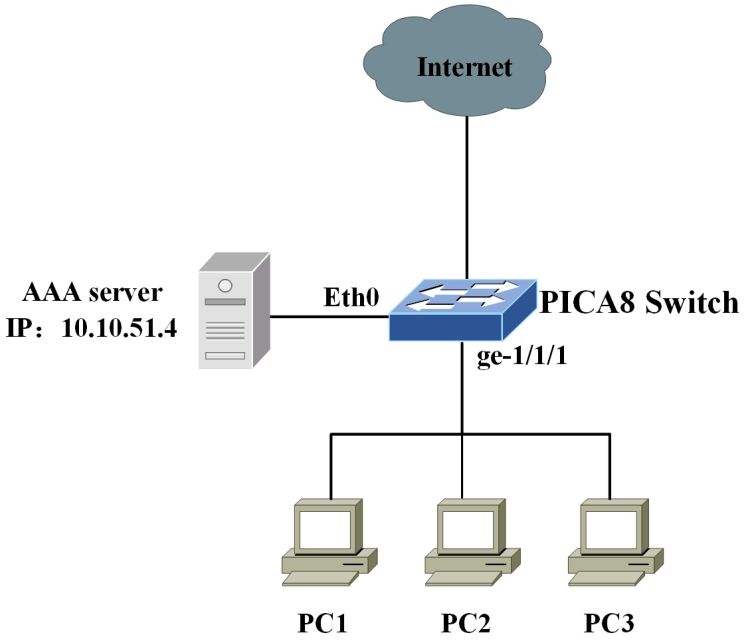
The configuration roadmap on the Web Authentication Server is as follows. For details, refer to the solution document Configuring Pica8 Switches with ClearPass Guest Central Web Authentication in Typical Configuration of NAC.

- Configure the Eth0 IP address of the switch to establish a connection to the switch.
- Configure the username and password on the AAA server for Web authentication.
- Configure a dynamic VLAN which is used to access the network normally after the user successfully authenticates.
- Configure other Web authentication attributes for Web authentication.

Configuration on the Switch

- Configure the 802.1X authentication server and Web authentication server on the Switch.
- The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, enable MAB authentication on the switch first.
- Configure block VLAN and dynamic VLAN.
- Configure CoA authorization client.

Figure 1. Networking Diagram for Configuring CWA Authentication



Procedure

Step1 Configure the access port to trunk mode.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
```

Step2 Configure the MAB and Web authentication modes. The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, enable MAB authentication on the switch first.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode web
```

Step3 Configure IP address of RADIUS server and the DNS server.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 10.10.51.4 shared-key pica8
```

```
admin@Xorplus# set system dns-server-ip 192.168.10.1
```

NOTE:

- Configuring DNS server IP is required for CWA authentication.
- Make sure to configure the mapping of the domain name of the redirect URL to the IP address on the DNS server.

Step4 Configure the NAS IP address to the IP address of Eth0 interface which is connected to the AAA server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 10.10.51.100
```

This command is used to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step5 Configure block VLAN. This step is required for Web authentication.

```
admin@XorPlus# set protocols dot1x block-vlan-id 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@XorPlus# set vlans vlan-id 10 l3-interface vlan10
admin@XorPlus# set l3-interface vlan-interface vlan10 address 10.10.51.10 prefix-length 24
```

Step6 Configure a RADIUS dynamic authorization client from which the switch accepts Change of Authorization (CoA) messages. This step is required for CoA and Web authentication.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1 shared-key pica8123
```

Step7 Configure the host mode for NAC authentication interface.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 host-mode multiple
```

Step8 Commit the configuration.

```
admin@Xorplus# commit
```

Step9 Verify the configuration.

a) After starting the browser and entering any Web address, the user is redirected to the Web authentication login page. Run command **run show dot1x interface gigabit-ethernet** *<interface-name>* to check the CWA authentication configurations.

```
admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/1
Interface ge-1/1/1:
============================================================
  Client MAC                : 10:11:01:39:1a:00
  Status                    : unauthorized
  Redirect URL              : https://www.clearpass.com/guest/weblogin.php/2?&mac=10:11:01:39:1a:00
============================================================
  Client MAC                : a1:31:a1:b9:6a:0c
  Status                    : unauthorized
  Redirect URL              : https://www.clearpass.com/guest/weblogin.php/2?&mac=a1:31:a1:b9:6a:0c
============================================================
  Client MAC                : a2:e1:55:78:1a:33
  Status                    : unauthorized
  Redirect URL              : https://www.clearpass.com/guest/weblogin.php/2?&mac=a2:e1:55:78:1a:33
============================================================
```

b) The user then enters the user name and password for authentication. If the user name and password are correct, an authentication success message is displayed on the Web authentication page. The user can then access the network.

c) Run the **run show dot1x interface** or **run show dot1x interface gigabit-ethernet** *<interface-name>* to check the CWA authentication configurations. The command output (**WEB = enable**) shows that the CWA authentication has been enabled on the interface ge-1/1/1 and MAC addresses 10:11:01:39:1a:00, a1:31:a1:b9:6a:0c and a2:e1:55:78:1a:33 are successfully authenticated.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x   MAC-RADIUS  WEB   HOST-MODE   Session-Timeout    CLIENT-MAC  CLIENT-STATUS
-------------------------------------------------------------------------------------------------------------
ge-1/1/1  disable  enable   enable   multiple(3)   0               10:11:01:39:1a:00  authorized
                                                                    a1:31:a1:b9:6a:0c  authorized
                                                                    a2:e1:55:78:1a:33  authorized

admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/1
```

```
Interface ge-1/1/1:
============================================================
  Client MAC               : 10:11:01:39:1a:00
  Status                   : authorized
  Success Auth Method      : MAB
  Dynamic VLAN ID          : 100 (active)
============================================================
  Client MAC               : a1:31:a1:b9:6a:0c
  Status                   : authorized
  Success Auth Method      : MAB
  Dynamic VLAN ID          : 100 (active)
============================================================
  Client MAC               : a2:e1:55:78:1a:33
  Status                   : authorized
  Success Auth Method      : MAB
  Dynamic VLAN ID          : 100 (active)
============================================================
```

Example for Configuring Multiple Authentication Modes

- Networking Requirements
  - Prerequisite
  - Configuration Roadmap on PICA8 Switch
- Procedure
- Verify the configuration

Networking Requirements

As shown in **Figure 1**, there are different types of terminal access the network in a company. For the security of the company network, the administrator needs to employ different types of NAC authentication modes on the access switch to control the access rights of different users.

Figure1. Topology for Configuring Multiple Authentication Modes

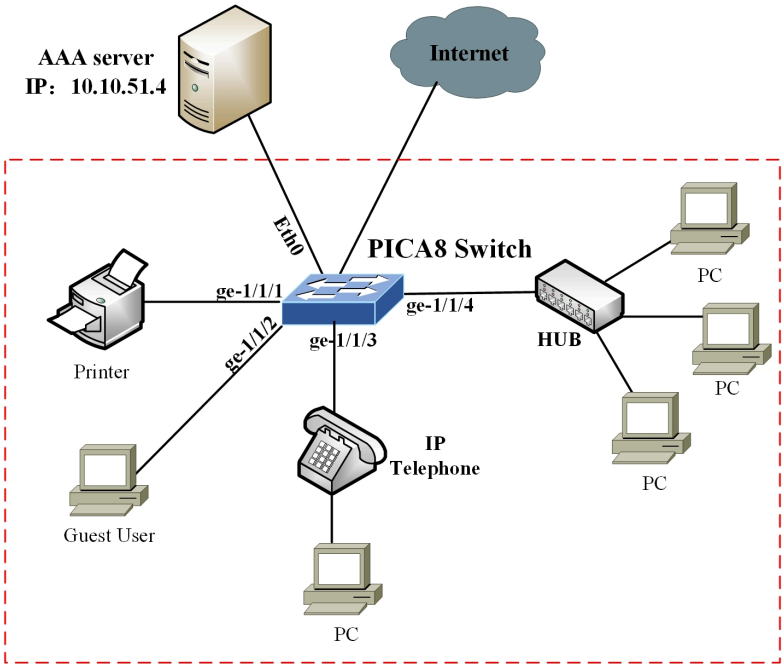


Figure 1 shows the topology for configuring multiple authentication modes. Follow the configuration roadmap below to complete the configuration.

Prerequisite

- Ensure that PICA8 Switch is properly connected to the AAA server. In this example, the switch uses the management port Eth0 to connect to the AAA server.
- Complete the NAC configurations on the AAA server. For details about how to configure NAC on AAA server, please refer to documents Typical Configuration of NAC.

Configuration Roadmap on PICA8 Switch

- A printer accesses the network through interface ge-1/1/1 of the switch. It is a dumb terminal and lacks the supplicant feature which is needed to pass on the 802.1X authentication credentials between the client and the authentication server. In this case, you can configure MAB authentication. You can use the **set protocols dot1x interface** *<interface-name>* **auth-mode mac-radius** command to enable MAB authentication mode on the interface.
- A guest user accesses the network through interface ge-1/1/2 of the switch, it doesn't have proper 802.1X or MAC Radius credentials saved on the authentication servers. In this case, you can configure CWA authentication to control the guest user's network access rights. Remember to enable MAB authentication before using CWA authentication.
- On interface ge-1/1/3, a PC and an IP telephone are connected to the switch so that both data and voice services can be transmitted.
  - Enable LLDP protocol for OUI learning from LLDP packets.
  - Configure 802.1X authentication on the ge-1/1/3 interface to perform access authentication on the connected PC.
  - Since there are two devices, a PC and an IP telephone, on port ge-1/1/3, you need to configure access port ge-1/1/3 for multiple host mode authentication.
  - It is strongly recommended not to use both voice VLAN and dynamic VLAN on the port enabled with NAC function. If both voice VLAN and dynamic VLAN are enabled on the port, dynamic VLAN A has a higher priority.
  - In this example, on the AAA server, you have to configure voice VLAN 300 for IP phone communication and dynamic VLAN 400 for data communication for the PC on the ge-1/1/3 interface.
  - On the switch, you need to use the **set vlans vlan-id** <vlan-id> command to create the dynamic VLANs in advance. And the link type of interface ge-1/1/3 should be configured as trunk port.
- Multiple PCs are connected to the switch on ge-1/1/4 interface. Enable 802.1X authentication on ge-1/1/4, and configure access port ge-1/1/4 for multiple host mode authentication.

Procedure

Step1 Create VLANs on the switch for dynamic VLAN.

```
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
```

Step2 Configure the access ports to trunk mode.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode trunk
```

Step3 Enable the authentication mode.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
admin@XorPlus# set protocols dot1x interface ge-1/1/2 auth-mode web
admin@XorPlus# set protocols dot1x interface ge-1/1/2 auth-mode mac-radius
admin@XorPlus# set protocols dot1x interface ge-1/1/3 auth-mode 802.1x
admin@XorPlus# set protocols dot1x interface ge-1/1/3 auth-mode mac-radius
admin@XorPlus# set protocols dot1x interface ge-1/1/4 auth-mode 802.1x
```

Step4 Configure IP address of AAA server, DNS server and CoA client.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 10.10.51.4 shared-key pica8
admin@XorPlus# set protocols dot1x aaa radius dynamic-author client 10.10.51.4 shared-key pica8
admin@Xorplus# set system dns-server-ip 192.168.10.1
```

Step5 Configure a block VLAN for CWA authentication.

```
admin@Xorplus# set protocols dot1x block-vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 200
admin@XorPlus# set vlans vlan-id 200 l3-interface vlan200
admin@XorPlus# set l3-interface vlan-interface vlan200 address 10.10.51.11 prefix-length 24
```

Step6 Configure the NAS IP address to the IP of the management interface eth0 which connected to the AAA server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 10.10.51.100
```

This command is to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the AAA server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step7 Configure the host mode for NAC authentication interface.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/3 host-mode multiple
admin@XorPlus# set protocols dot1x interface ge-1/1/4 host-mode multiple
```

Step8 Enable LLDP protocol for OUI learning from LLDP packets.

```
admin@XorPlus# set protocols lldp enable true
```

Step9 (Optional) Enable PoE function on the interface ge-1/1/3 if the IP telephone obtains power through the PoE port of the switch.

```
admin@XorPlus# set poe interface ge-1/1/3 enable true
```

Step10 Commit the configuration.

```
admin@XorPlus# commit
```

Verify the configuration

a) Run the **run show dot1x interface** or **run show dot1x interface gigabit-ethernet** <*interface-name*> to check the NAC authentication configurations. The command output shows that the NAC authentication has been enabled and the terminals are successfully authenticated on each port.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x   MAC-RADIUS  WEB     HOST-MODE   Session-Timeout    CLIENT-MAC  CLIENT-STATUS
-------------------------------------------------------------------------------------------------------------
ge-1/1/1   disable  enable      disable      single(1)    0    f8:9e:01:9e:cc:a1    authorized
ge-1/1/2   disable  enable      enable       single(2)    0    23:5e:81:77:ac:a2    authorized
```

```
ge-1/1/3   enable   enable      disable      multiple(2)  0    ad:ee:02:45:d3:a3    authorized
                                                              6d:33:12:4b:ef:a4    authorized
ge-1/1/4   enable   enable      disable      multiple(3)  0    f2:3e:00:8a:90:a5    authorized
                                                              a2:44:00:5a:90:3d    authorized
                                                              56:33:a0:ee:f0:ab    authorized


admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/3
Interface ge-1/1/3:
============================================================
  Client MAC               : ad:ee:02:45:d3:a3
  Status                   : authorized
  Success Auth Method      : MAB
  Traffic Class            : Voice
  Dynamic VLAN ID          : 300 (active)
============================================================
  Client MAC               : 6d:33:12:4b:ef:a4
  Status                   : authorized
  Success Auth Method      : MAB
  Traffic Class            : Other
  Dynamic VLAN ID          : 400 (active)
============================================================
```

b) Use run show lldp neighbor command to check the LLDP neighbor information on interface ge-1/1/3.

```
admin@Xorplus# run show lldp neighbor
LLDP Remote Devices Information
LocalPort   ChassisId                PortId             Management Address  System Name      Platform           Ca
----------  -----------------------  -----------------  ------------------  ---------------  -----------------  --
ge-1/1/3    3C:2C:99:41:47:E1        ge-1/1/13          10.10.51.100        Xorplus          as4610_30t         B
```

c) The terminal can access the network after passed the corresponding authentication method.

Typical Configuration of NAC

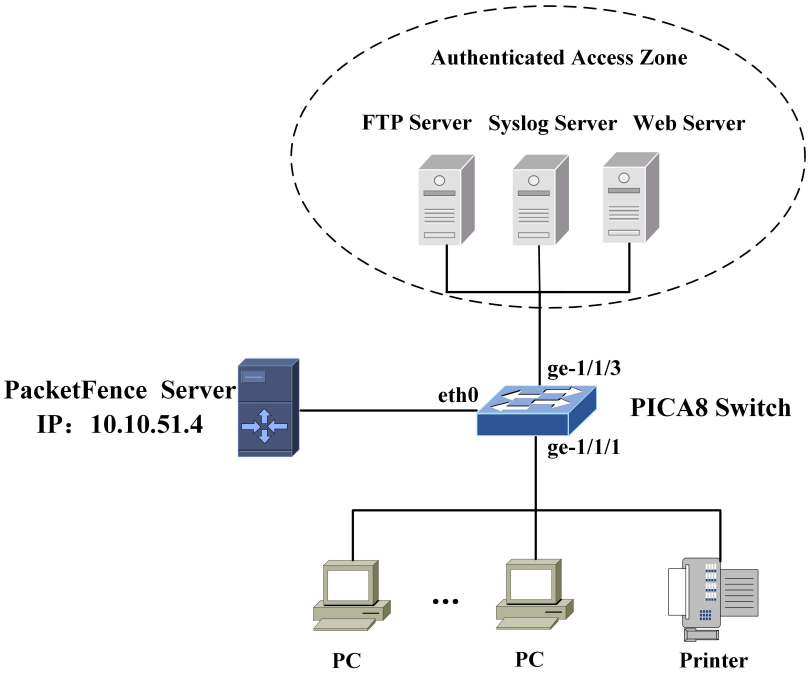
- Example for Configuring NAC (PacketFence as the Authentication Server)
- Solution Documents Download

Example for Configuring NAC (PacketFence as the Authentication Server)

Networking Requirements

As shown in **Figure 1**, a large number of user terminals access the Authenticated Access Zone of a company through ge-1/1/1 of the PICA8 Switch (as the access device). If the user terminals are not authenticated, any visitor may easily steal the company's confidential information or attack the company's intranet, resulting in an insecure intranet.

Figure 1. Networking Diagram for Configuring 802.1X Authentication



To ensure network access security, the administrator employs 802.1X authentication on the Switch and PacketFence server, to control the network access of the user terminals. The Switch allows the user terminals to access resources in the Authenticated Access Zone only when the 802.1X authentication is successfully passed.

There are both PCs and dumb terminals, such as printers and IP phones, connected to the enterprise network. In order to flexibly adapt to different authentication requirements from different access terminals in the user environment, both 802.1X authentication and MAB authentication should be deployed on the PICA8 access switch. Users can access the network through either 802.1X or MAB authentication, or both authentication modes.

Basic Configuration Plan

Table 1. PICA8 Switch Data Plan

Items	Data	Description
PICOS version	PICOS: 2.11.22	-
PacketFence server IP address	192.168.10.7	-
Shared-key	pica8	Make sure you enter the same secret key as shared-key on the PacketFence server when adding a PICA8 switch in PacketFence database.
Authentication mode	802.1x mac-radius	Enable both 802.1X and MAB authentication methods.
RADIUS dynamic authorization client for Change of Authorization (CoA)	192.168.10.7	-

Table 2. PacketFence Server Data Plan

Items	Data	Description
Switch IP address	192.168.10.10	The IP address of ge-1/1/2 on PICA8 switch, using in-band communication.
Access user	Username: pica8 Password: Pica8pica8	**Note:** Ethernet-EAP connection type means the client is connecting using 802.1X credentials.
	Connection Profile : Connection Type = Ethernet-EAP Sources: local	
MAC address of the connected dumb terminal device	MAC address: 00:00:06:00:00:07	No need to specify a username and password for MAC authentication in PacketFence database (the node's MAC address is used by the switch as the username and password when sending an Access Request on behalf of the client).
	Connection Profile : Connection Type=WIRED_MAC_AUTH	
RADIUS secret key	pica8	Make sure you enter this same secret key as shared-key on the switch when configuring 802.1X protocol on PICA8 switch.
RADIUS authentication methods	**MSCHAPv2** and **PEAP**	On the client side also set **PEAP** and **MSCHAPv2** for 802.1X configuration.

Configuration Notes

- The shared key must be consistently configured on PICA8 switch and the PacketFence server.
- On the client side also set **PEAP** and **MSCHAPv2** for 802.1X configuration which is same to the RADIUS authentication methods on PacketFence server.
- Make sure the 802.1X client software is installed and enabled on the client device.

Configuration Roadmap

1. Configure PICA8 Switch, including the VLAN to which the access interface belongs, parameters for connecting to the PacketFence server, and enabling 802.1X and MAB authentication.

> **NOTE:**
> Make sure network connection between PICA8 Switch and the PacketFence Server is reachable.

2. Configure the PacketFence server:
    a. Log in to the PacketFence server.
    b. Add a switch to the PacketFence server.
    c. Add a user and node to the PacketFence server.
    d. Add the secret key and Radius Authentication Methods on the PacketFence server.
    e. Packetfence configuration file changes and miscellaneous configurations.

Procedure

PICA8 Switch Configuration

Step1 Configure the VLAN interface.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 200
admin@XorPlus# set vlans vlan-id 100 l3-interface vlan100
admin@XorPlus# set vlans vlan-id 200 l3-interface vlan200
admin@XorPlus# set l3-interface vlan-interface vlan100 address 192.168.10.10 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan200 address 192.168.20.10 prefix-length 24
```

Step2 Configure IP address of PacketFence server and the shared key.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 192.168.10.7 shared-key pica8
```

Step3 Configure the NAS IP address to the L3 VLAN interface IP which connected to the RADIUS server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 192.168.10.10
```

This command is to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step4 Enable 802.1X and MAB authentication mode on interface ge-1/1/1.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
```

Step5 Configure the host mode to multiple for the interface ge-1/1/1.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 host-mode multiple
```

Step6 (Optional) Configure a RADIUS dynamic authorization client from which the switch accepts Change of Authorization (CoA) messages.

```
admin@XorPlus# set protocols dot1x aaa radius dynamic-author client 192.168.10.7 shared-key pica8
```

Step7 Commit the configuration.

```
admin@Xorplus# commit
```

PacketFence Configuration

Step1 Login to the PacketFence server.

a) Go to Web login page at: https://*server-ip*:1443/admin/

b) Enter Username/password and click login. (You setup username/password during initial configuration of PacketFence)

Step2 Add a switch to the PacketFence server.

a) Click **Configuration** > **Switches** > **ADD SWITCH** > **default**.

b) Add switch with the switch IP address: 192.168.10.10.

c) Choose type as **Pica8** and mode as **production**.

d) Click on **Radius** tab and enter secret key. Make sure you enter this same secret key as shared-key on the switch when configuring 802.1X protocol on PICA8 switch.

e) Click on the Roles tab, make sure the Role mapping by VLAN ID is checked, also define your roles and the corresponding VLANs should be defined here.

f) For the **Deauthentication Method**, select RADIUS.

g) Make sure the **use CoA** box is checked.

h) Leave all other configuration as they are (default) and click Save to add the switch to PacketFence database.

Refer to **Figure 2** which illustrates adding a new switch to PacketFence.

Figure 2. Add PICA8 switch to PacketFence

Step3 Add a User to PacketFence Database.

For 802.1X authentication , we must first add all our users to the PacketFence database. The username and password are the two most important attributes in 802.1X authentication. We must make sure that username and password sent in the Access-Request by clients matches an entry in the PacketFence database otherwise 802.1X authentication won't be successful. Follow the steps below to add a User to PacketFence.

a) Click on **USERS** > **Create**.

b) Enter username, password and email address for this user.

c) You can enter other user details as per requirement like Firstname, Company etc.

d) Enter the time in **Registration Window** (mandatory).

e) In Action, Choose **Role** and then select a proper role for this user.

f) Choose appropriate access duration (mandatory).

g) Click **CREATE USERS** to save the user to PacketFence.

Refer to **Figure 3** below for an illustration.

Figure 3. Adding a User in PacketFence

Step4 Add a connection profile in Packetfence.

a) Click on **CONFIGURATION > Connection Profiles > ADD PROFILE**.

b) Give it any name and description, say dot1x.

c) Add a filter in dot1x profile, If Any,... Connection Type = Ethernet-EAP.

d) Choose sources as **local**.

e) For **Device registration** select default.

f) Leave the remaining options as they are (default values).

g) Click **Save** to save your changes.

Note: Ethernet-EAP connection type means the client is connecting using 802.1X credentials.

The above Connection Profile would be activated whenever 802.1X authentication requests are received at the PacketFence server.

Refer to **Figure 4** for illustration.

Figure 4. Adding a Connection Profile

Step5 Configure PacketFence for MAC Authentication.

For MAC authentication we need to perform the following steps:

a) Add a node to the PacketFence database (similar to how we add a node for 802.1X Authentication).

b) Add the MAC address: 00:00:06:00:00:07. Note: No need to specify a username and password for MAC authentication in PacketFence database (the node's MAC address is used by the switch as the username and password when sending an Access Request on behalf of the client).

c) Add a connection profile for MAC authentication. Even though we can have a single Connection Profile for both 802.1X and MAC authentications, it would be however, better if we have separate Connection Profile for the two different types of authentications. To add a MAC authentication profile follow the procedure mentioned in the 802.1X section of adding a Connection Profile with the exception of **Connection Type** in **Filter.** While adding a Connection Profile for MAC authentication, choose Connection Type as **WIRED_MAC_AUTH.** The rest of the procedure is same as that of the 802.1X.

Step6 Configure Radius Authentication Methods in Packetfence.

a) Click on **CONFIGURATION > System Config (bottom item on far left) > Authentication Methods**.

b) For EAP Auth Type, remove all methods except **MSCHAPv2** and **PEAP**, you can add **MD5** here as well if you wish to use MD5 with 802.1X.

c) Click **SAVE**.

d) On the client side also set **PEAP** and **MSCHAPv2** for 802.1X configuration.

Refer to **Figure 5** below for illustration.

Figure 5. Configuring Radius Authentication Methods

Step7 Miscellaneous configurations.

a) We need to change or set the way how PacketFence stores passwords in its database. For PICA8 switches, we need to save user passwords as plaintext. To achieve this follow the steps below:

Click on **Configuration > System Config > >dvanced > Database passwords hashing method >** choose **plaintext**.

b) To enable radius communication on the management interface we need to make the following changes to ensure radius messages are accepted on the management interface.

Click on **Configuration > Network Configuration > Interfaces >** click **eth0 > Type** = **Management**.

For the **Additionnal listening daemon**(s) choose **radius**.

Step8 Packetfence configuration file changes.

a) To allow local authentication with radius integrated with packetfence, uncomment the line *packetfence-local-auth* in **/usr/local/pf/conf/radiusd/packetfence-tunnel**.

b) To allow EAP-MD5 authentication, add **packetfence-eap-mac-policy** line just before **packetfence-eap-mac-policy** in file **/usr/local/pf/conf/radiusd/packetfence**

Note: It is recommended to use PEAP for 802.1X authentication as it is considered more secure compared to MD5.

Verify the Configuration

- Run the **run show dot1x interface** and **run show dot1x mab** command to check the 802.1X and MAB authentication configurations. The command output (**PortEnabled = true**) shows that the 802.1X authentication has been enabled on the interface ge-1/1/1 and MAC address 00:00:06:00:00:07 is successfully authenticated.

```
admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/1
Interface ge-1/1/1:
============================================================
  Client MAC              : 00:00:06:00:00:07
  Status                  : authorized
  Success Auth Method     : 802.1x
  Dynamic VLAN ID         : 200 (active)
============================================================
Client MAC                  : e0:db:55:cd:84:62
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
============================================================
```

- The user starts the 802.1X client software on the terminal, enters the username and password, and starts authentication.
- If the user name and password are correct, there will be an authentication success message displayed. Then users can access the network through this port.

Appendix

A sample configuration file of the switch when using the out-of-band (OOB) management port (i.e. eth0) to connect to PacketFence is provided here.

```
# ge-1/1/11 and ge-1/1/13 are the access ports which have enabled 802.1x authentication.
  set interface gigabit-ethernet ge-1/1/11 family ethernet-switching port-mode "trunk"
  set interface gigabit-ethernet ge-1/1/13 family ethernet-switching port-mode "trunk"
  set protocols dot1x interface ge-1/1/11 auth-mode "mac-radius"
  set protocols dot1x aaa radius authentication server-ip 10.10.53.234 shared-key "test"
  set vlans vlan-id 10
  set vlans vlan-id 20
  set vlans vlan-id 30
```

Solution Documents Download

- Integrating Pica8 Switches with Cisco ISE.docx
- Configuring Central Web Authentication with Pica8 Switches and Cisco ISE.docx
- Integrating Pica8 Switch with ClearPass.docx
- Windows User and Machine Authentication with ClearPass.docx
- ClearPass Integration with Active Directory and Pica8 Switches.docx
- Configuring Pica8 Switches with ClearPass Guest Central Web Authentication.docx
- Configuring Dynamic and Downloadable ACL on Cisco ISE.docx
- Configuring Dynamic and Downloadable ACL for ClearPass.docx

References

The standards of NAC authentication are described in the following table.

Document	Description
RFC5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
RFC3748	Extensible Authentication Protocol (EAP)
RFC3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
RFC4672	RADIUS Dynamic Authorization Client MIB
IEEE Std 802.1X-2004	Port Based Network Access Control

Principle of NAC

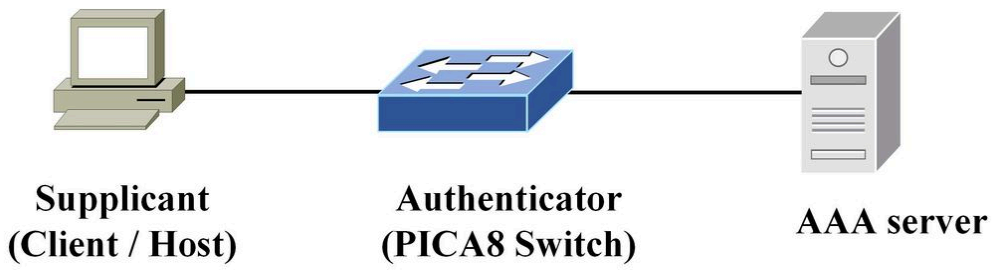
- Introduction to NAC Authentication
  - Host Mode
  - Server Fail VLAN
  - Block VLAN and Dynamic VLAN
  - Fallback to WEB Function
  - Comparison of the Three Authentication Modes
- 802.1X Authentication
  - EAP Packet Exchange Process
  - Authentication Trigger Types
- MAC Authentication Bypass (MAB) Authentication
- Central Web Authentication (CWA)
  - Introduction
  - Redirect URL
  - CWA Authentication Process
- RADIUS Accounting for 802.1X and MAB
- Change of Authorization (CoA)
- Downloadable ACL
  - NOTE:
- Dynamic ACL
- Response to session-timeout Attribute
- Vendor Specific Attribute (VSA)
  - How to Import PICA8 RADIUS Dictionary to ClearPass
  - How to Import PICA8 RADIUS Dictionary for Cisco ISE
  - How to Import PICA8 RADIUS Dictionary to FreeRadius server

Introduction to NAC Authentication

Network Access Control (NAC) is a network access security function which controls the user authentication and access to the network resources through the access port.

As shown in **Figure 1**, the NAC authentication system is a typical Client/Server architecture which involves three components: Supplicant, Authenticator and AAA server.

Figure 1. Architecture of the NAC Authentication System



- **Supplicant**: The supplicant is the user device that wants access to the network resources through the switch. It is a client or a host that provides the user name and password to the authentication server to obtain network access rights.

- **Authenticator**: The PICA8 Switch functions as the authenticator in the NAC authentication system. As an authentication gateway device, PICA8 Switch transfers authentication information between the client and the authentication server, and controls network access and authorization of the client.
- **AAA server**: The authentication server is the entity that validates authentication credentials provided by the supplicant. RADIUS is a commonly used authentication server. The administrator configures the user's authentication and authorization information on the AAA server that is used to validate the client in the NAC authentication process and determine whether the client can access the network resources.

> **NOTE:**
>
> - The administrator needs to configure both the AAA server and PICA8 switch to deploy the NAC function successfully.
> - From PICOS version 2.11.22, the NAC authentication function is extended to support Web authentication, downloadable ACL and dynamic ACL.

Host Mode

Host Mode refers to whether a single or multiple clients are allowed access on a single switch port. PICOS NAC function is a combination of switch port and the client's MAC address learned on that switch port to implement user access control. Each switch port can be configured to operate in either **single** or **multiple** host mode**.**

- **single:** Only one user is allowed access to the switch port, unless the user goes offline other users will not be allowed access to the network. The authentication process will be reinitiated if the port is bounced or client is changed.
- **multiple:** Multiple clients connect to the network through the same switch port. If a user goes offline, the network access rights of other users are not affected. At most 8 clients are allowed to be authenticated on a single switch port, the ninth will be added into the pending list.

You can set the host mode of the interface by using command **set protocols dot1x interface** <*interface-name*> **host-mode** <**single** | **multiple**>. The default host mode is **single**. Note that changing host mode from CLI will cause re-authentication for all connected users of the port.

Server Fail VLAN

The purpose of a server fail VLAN is to provide limited network connectivity to users in the event of AAA server failure or unreachability. After a RADIUS server is configured, the switch sends Test Radius Request message to the server to detect the reachability of the RADIUS server. If all the RADIUS servers are unreachable, the port connected to the client will be added to the server fail VLAN, and the packets from the client can be forwarded in server fail VLAN. The switch continues to send the detection packets every second for 3 times (can be set by CLI command) to check whether the server is reachable. If one of the RADIUS servers is reachable, the switch removes this client from the server fail VLAN and adds it back into the block VLAN, and the switch stops sending the detective packets.

Users can use the **set protocols dot1x server-fail-vlan-id** <*vlan-id*> command to specify a server fail VLAN, the **run show dot1x server** command can be used to show the reachability of each RADIUS servers configured on the switch, **run show dot1x all** command can be used to view the NAC configuration information, including the server fail VLAN.

For example,

```
admin@Xorplus# run show dot1x server
Server-IP         Status        Priority  Retry-Interval  Retry-Num   Detect-Interval   Consecutive-Detect-Num
---------------   -----------   --------  --------------  ---------   ---------------   ----------------
10.10.51.70       reachable     2          5   Sec(s)      5          5   Sec(s)         8


admin@Xorplus# run show dot1x all
Global-Info:
--------------------------------------------------------------------------------
NAS-IP           :  10.10.1.1
```

```
Block-VLAN         :  2
Block-VLAN-IP        :  172.16.1.1/24
WEB-AUTH-MODE           :  Remote
Server-Fail-VLAN      :  100
--------------------------------------------------------------------------------
```

NOTE:

A maximum of 20 RADIUS servers can be configured on the switch. The reachable server with the smallest IP address will be used for NAC authentication.

Block VLAN and Dynamic VLAN

Block VLAN is a global configuration for NAC authentication. The port enabled with web authentication NAC feature will be added to the block VLAN automatically. Users in the block VLAN have very limited access network resources before being authenticated successfully through the web authentication portal. Block VLAN is a mandatory prerequisite for web authentication. If block VLAN is not specified, the switch won't allow the user to configure web authentication for any physical port.

The switch will move the clients from the block VLAN to an AAA server specified dynamic VLAN after successful authentication. If the RADIUS authentication server does not deliver a dynamic VLAN, then the client is moved to the native VLAN of the interface.

When configuring dynamic VLAN, you need to pay attention to the following points:

- On the switch, you need to use the **set vlans vlan-id** <*vlan-id*> command to create a dynamic VLAN in advance. And the link type of the port should be configured as trunk port.
- On the AAA server, you need to configure and deliver a dynamic VLAN. When configuring the dynamic VLAN, dynamic VLAN name is a string type, and its length must be less than or equal to 10 characters.
- Dynamic VLAN and block VLAN cannot be the same VLAN.

The L3 VLAN interface should be enabled on the block VLAN. The IP address of this VLAN-interface should be configured to establish a temporary connection between the user and the switch to complete the subsequent Web authentication process.

After creating a block VLAN, you can use the **run show vlans** command to view VLAN information.

NOTE:

When deploying voice VLAN feature together with NAC feature, pay attention the following points:

- It is strongly recommended not to use both voice VLAN and dynamic VLAN on the port enabled with NAC function, as this may cause voice traffic to be blocked.
- If the returned RADIUS access accept message includes an extra Pica8 vendor-specific-attribute (VSA)"pica8-traffic-class=voice", the dynamic VLAN will take precedence over the locally configured voice VLAN when making LLDP negotiation. If you want to transmit voice traffic through dynamic VLAN, please configure and deliver this VSA on AAA server.

Fallback to WEB Function

PICOS NAC function includes three authentication modes: 802.1X authentication, MAB authentication and Central Web Authentication (CWA). To use NAC to control users' network access rights, you must enable one or more authentication modes on a switch interface. Note that: CWA authentication process relies on MAB authentication. If you want to deploy CWA, you need to enable MAB authentication first.

PICOS supports fallback to WEB if 802.1X authentication fails. This function controls whether MAB authentication is performed when 802.1X authentication fails. Enabling or disabling fallback to WEB function leads to two different results.

1. Fallback to WEB function is disabled. This is the default configuration.

- When both 802.1X authentication and MAB authentication modes are enabled, the 802.1X authentication will take precedence over MAB.

If the Supplicant supports 802.1X authentication, the system performs 802.1X authentication. If the Supplicant does not support 802.1X authentication, the system performs MAB authentication.

For the former case, irrespective of whether 802.1X authentication is successful or not, MAB authentication will not be performed. It's important to note here that if the client sends in 802.1X credentials and the authentication fails for some reason, the switch will not initiate MAB authentication in case where both 802.1X and MAB are configured for the switch port.

If the 802.1X authentication fails, the switch will try the authentication process maximum of three times. If the authentication fails after trying three times, the switch will ignore any more request from the client in the EAP_TIME_OUT time (60 seconds) which is called a quiet time before the switch initiates re-authentication.

- If all three modes are enabled, the system considers 802.1X authentication and MAB authentication as described above. If the 802.1X authentication is not supported and the MAB authentication fails, the system will perform the CWA authentication mode for the client.

2. Fallback to WEB function is enabled.

- When both 802.1X authentication and MAB authentication modes are enabled, the 802.1X authentication will take precedence over MAB.

If the Supplicant supports 802.1X authentication, the system performs 802.1X authentication. If the Supplicant does not support 802.1X authentication, the system performs MAB authentication.

For the former case, if the 802.1X authentication fails, the system tries to perform MAB authentication. This is different from the scenarios when fallback to WEB function is disabled. Note that: It will not take dot1x authentication if already fallback to CWA until MAC ages out and learns again by cable plugging in/out or MAC address clearing.

- If all three modes are enabled, at first, the system considers 802.1X authentication and MAB authentication as described above. If the 802.1X authentication is not supported and the MAB authentication fails, the system will perform the CWA authentication mode for the client.

Comparison of the Three Authentication Modes

The application scenarios of the three authentication modes are different, the below table compares the three authentication modes.

Items	802.1X Authentication	MAB Authentication	CWA Authentication
Client Software	The 802.1X client software is required to be installed on the supplicant device.	Not required.	The supplicant needs to install a Web browser.
Characteristics	The Extensible Authentication Protocol (EAP) is used to exchange authentication information between the client, the switch and the authentication server. High security.	Complex management as it requires registering each MAC address on the AAA server.	Flexible deployment.
Scenarios	Applicable to scenarios where requirements for security are high.	Can be deployed in scenarios where 802.1X cannot be deployed. Authentication of dumb terminals such as printers and fax machines.	Applicable to temporary access or guest access scenarios.

802.1X Authentication

802.1X authentication is an authentication method that controls the network access rights of users based on the switch port and the MAC addresses of clients learned on that port. The Extensible Authentication Protocol (EAP) packet is used to exchange authentication information between the supplicant, authenticator and authentication server. This technology is mainly used in networks with high security requirements. 802.1X authentication requires 802.1X client software to be installed on the supplicant.

You can use the **set protocols dot1x interface** <*interface-name*> **auth-mode 802.1x** command to enable 802.1X authentication mode on an interface.

EAP Packet Exchange Process

The EAP packet exchange process is described as follows:

1. The EAP packets transmitted between the authenticator and supplicant are encapsulated in EAPOL format and transmitted across the LAN.
2. The authenticator and authentication server (a RADIUS server) exchange EAP packets in EAP relay mode. The authenticator encapsulates EAP packets in EAP over RADIUS (EAPOR) format and sends the packets to the RADIUS server for authentication. This authentication mode supports various EAP authentication methods, such as MD5- Challenge, EAP-TLS, and PEAP. However, the RADIUS server is required to support the corresponding EAP authentication methods. The credentials can be based on username/password or the certificate-based. You need to follow the configuration guide in this document to employ 802.1X authentication based on the username/password. However, certificate-based authentication does not need to do any configuration on the switch.

Authentication Trigger Types

The 802.1X authentication process can be initiated by either the client or the access device in the following two types:

- Triggered by the client

The client sends an EAPOL-Start packet to the access device to trigger authentication. The destination address of the packet is a multicast MAC address assigned by the IEEE 802.1X protocol: 01:80:C2:00:00:03.

- Triggered by the access device

For clients that cannot send EAPOL-Start packets proactively, the access device supports proactive trigger of the 802.1X authentication.

The access device sends a multicast EAP-Request/Identity packet to the client with the multicast MAC address 01:80:C2:00:00:03 to trigger 802.1X authentication every 30 seconds.

MAC Authentication Bypass (MAB) Authentication

Not all the network devices support 802.1X, such as a printer, camera, or a wireless phone. Such devices lack the supplicant feature which is needed to pass on the 802.1X authentication credentials between the client and the authentication server.

In this case, you can use MAC Authentication Bypass (MAB) function to authenticate network devices. You can use the **set protocols dot1x interface** <*interface-name*> **auth-mode mac-radius** command to enable MAB authentication mode on an interface.

When the interface enabled with MAB authentication learns the MAC address of the user, PICOS will perform the MAB authentication process. During the authentication process, the user is not required to manually enter a username or password. The user's MAC address will be encapsulated as the user-name and password in a RADIUS Access Request packet and sent to the AAA server. The port will be opened to the user with this MAC address only if MAB authentication is passed successfully. This technology is suitable for environments where the MAC address is fixed and the security requirements are not very high. At the same time, it can meet the authentication requirements of terminals such as printers that cannot install the 802.1X authentication client software.

When the MAC entry is aged or deleted, the user session with this source MAC will be disconnected. MAB authentication will be performed again if the user wants to access the network resources through this port.

Central Web Authentication (CWA)

Introduction

Central Web Authentication (CWA) provides a means to enterprise network administrators to allow guests on the network some form of access to network resources, which is also referred to as Web authentication. This feature is particularly helpful because guest users usually do not have proper 802.1X or MAC Radius credentials saved on the authentication servers.

With Web authentication feature, PICA8 switches can now provide an additional feature to guest users to use their web browser to access a login page where they can provide either authentication credentials for guests or simply accept a use-policy to access the network. In centralized web authentication environment, the PICA8 switch works as a proxy between the authentication server and user. When the user connects to the network and tries to access a Web page, the user is redirected to the authentication page on the Web authentication server. Only after entering the correct username and password can the user successfully access the network resources.

You can use the **set protocols dot1x interface** <*interface-name*> **auth-mode web** command to enable WEB authentication mode on an interface.

NOTE:

- The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, enable MAB authentication on the switch first.

Ø From CLI configuration, you need to enable MAB authentication before enabling CWA authentication.

Ø The CWA authentication works in conjunction with MAB authentication. The CWA authentication process will be implemented after the MAB authentication fails.

- To implement CWA authentication, there are a series of configurations on both the switch and AAA server, for details of how to configure CWA, please refer to section Example for Configuring CWA Authentication and the solution documentation Configuring Pica8 Switches with ClearPass Guest Central Web Authentication in Typical Configuration of NAC.
- Both L2 and L3 connections between the client and the switch are supported when deploying CWA authentication.

Redirect URL

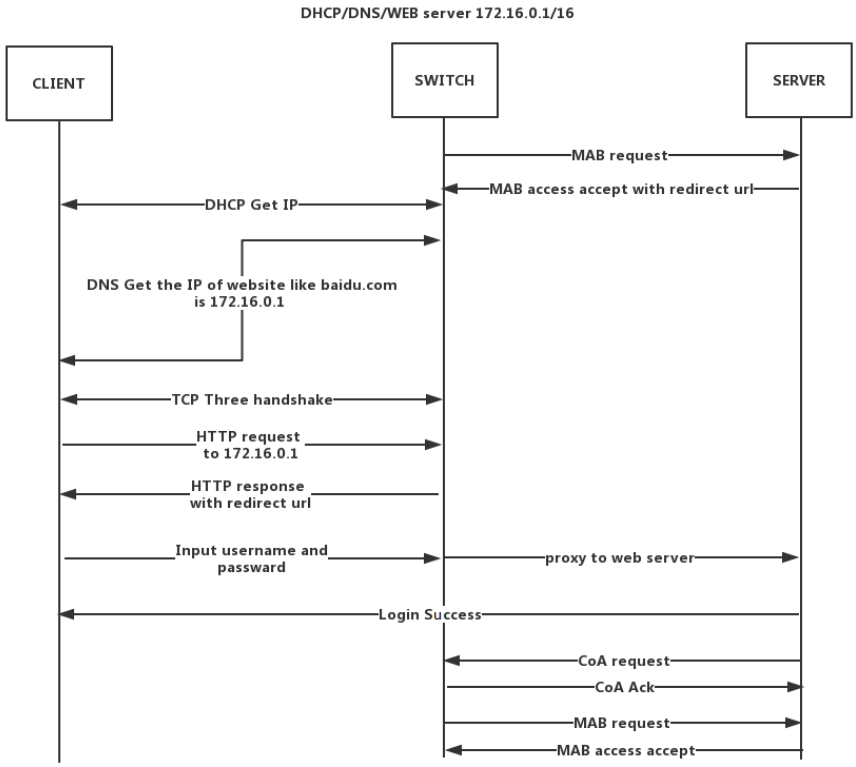
In the CWA authentication process, when the user connects to the network and tries to access a web page, the user is redirected to the authentication page on the web authentication server. Only after entering the correct username and password can the user successfully access the network resources.

The Redirect URL is a vendor-specific attribute (VSA) of type string defined on the AAA server. The attribute name is **Pica8-Redirect-URL** and the attribute ID number is **4** in the PICA8 RADIUS dictionary. To use the Redirect URL VSA the user has to import PICA8 RADIUS dictionary to AAA server. For details about how to import PICA8 RADIUS dictionary, please refer to the document How to Import PICA8 RADIUS Dictionary.

CWA Authentication Process

Figure 2 shows the CWA authentication process.

Figure 2. CWA authentication process



1. The client is connected to the switch port and its MAC address is learned by the switch. The switch sends an MAB Request message to the AAA server to initiate MAB authentication for the guest user. The message carries the MAC address of the client as the authentication username and password.
2. As the client's MAC address is an unregistered address on the AAA server, the MAB authentication fails. However, the AAA server is configured in such a way that an Access-Accept message is sent to the switch with a redirect URL for unregistered users.
3. The client interacts with the switch to obtain a temporary IP address from the DHCP server running in the block VLAN.
4. DNS resolution is done locally on DNS server running on the switch. Domain names such as www.example.com are resolved to the block VLAN interface IP address (e.g. 172.16.0.1) instead of its actual IP address. It’s important to note that both the DNS and DHCP server have the same IP address as the block VLAN interface IP address of 172.16.0.1.
5. The client and the switch perform a TCP three-way handshake to establish a TCP connection.
6. Then the client opens a web browser, initiates an HTTP access request.
7. The switch replies to the client with the redirect URL in the HTTP response. The Switch gets the IP address of CWA server (is included in the re-directio URL) resolved by the configured DNS.
8. The client’s request is redirected to the redirect URL page on the AAA server that requires the client to enter the username and password.
9. After the client enters the correct username and password, login succeeds. AAA server sends a CoA bounce-port command to the switch.
10. The switch and AAA server perform MAB authentication on the client MAC address again. This time the client is a known client to the AAA server, so another Access-Accept message is sent along with a dynamic VLAN ID. The switch port is then put into the dynamic VLAN.
11. MAB authentication and Web authentication succeed. The user can access the Web resources normally.

RADIUS Accounting for 802.1X and MAB

> **NOTE:**
>
> RADIUS accounting applies only to 802.1X and MAB authentication procedures.

Enterprises or carriers need to charge users who are accessing different enterprise or carrier services such as Internet to be able to accurately and effectively calculate billing information for their customers

When a user gets online, the switch will send accounting start message to the AAA server when authentication is passed and starts accounting; When the user gets offline by either MAC aged out or be deleted, the switch will send accounting stop packet to the AAA server to stop accounting. In the accounting stop packet, the attribute Acct-Session-Time carries the amount of time the user was online.

Users can use the **set protocols dot1x aaa radius accounting disable** <**true | false**> command to enable or disable accounting function for 802.1X and MAB.

AAA server records the packet consumption, you can use the command **run show dot1x dynamic/downloadable filter** to check the counter result. For example,

```
admin@Xorplus# run show  dot1x downloadable filter
  ------------------------------------------------------------
  Downloadable Filter Name : abc
  Applied Interface              : ge-1/1/25
  Applied Client MAC             : 00:00:00:00:11:22
  Downloadable Filter Rule : sequence 500 from destination-address-ipv4  192.168.2.0/24
                             sequence 500 then action forward
  Downloadable Rule Counter: sequence 500       match counter: 115595648 packets
```

```
admin@Xorplus# run show dot1x dynamic filter
==========================================================================
    Filter: f6
      Description     :
      ------------------------------------------------------------
      Sequence        : 50
      Description     :
      Match counter   : 60544 packets
      Match Condition : Destination MAC     : 00:00:00:88:88:88
      Action          : Forward
      ------------------------------------------------------------
      Applied Clients : ge-1/1/25    00:00:00:00:11:22
```

Change of Authorization (CoA)

Server initiated Change of Authorization allows the administrator to modify the authorization of the already authorized users through the CoA messages from the AAA server.

The AAA server sends CoA messages to the PICA8 switch when the authorization information of an authorized user is changed by the administrator. The switch initiates a new authorization of the client when it receives a CoA messages. For example, if the administrator configures to disable the host port on the AAA server, the AAA server will send a CoA-Request message with disable-host-port field to the switch to disable the port connecting to the host.

CoA involves two parties: Dynamic Authorization Server (DAS) and Dynamic Authorization Client (DAC):

- DAS: The component that resides on the NAS (switch) that processes and replies to the Change-of-Authorization (CoA) Request and Disconnect messages.
- DAC: The component that sends CoA-Request and Disconnect messages to the Dynamic Authorization Server. This component often resides on the RADIUS server. For details, please refer to RFC5176.

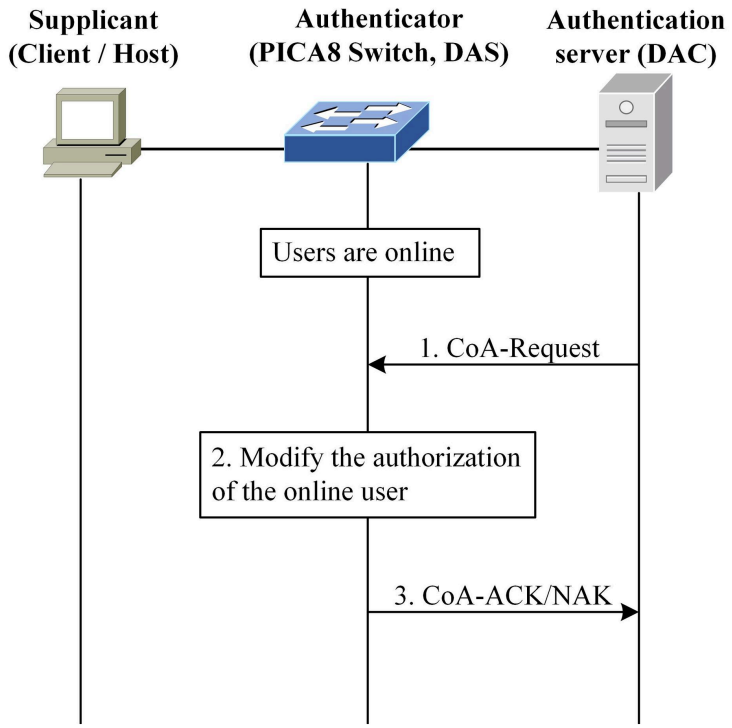
> **NOTE:**

- The CoA feature provides network administrators the flexibility to remotely control authorization changes of clients.
- FreeRADIUS server does not support DAC function. To support DAC function, user needs to connect to an AAA platform that supports DAC of CoA function, such as PacketFence.
- PICOS supports to configure a maximum of 20 CoA dynamic authorization clients.

CoA includes two types of message flows: Disconnect and Change-of-Authorization (CoA) processes. Disconnect message terminates a user session immediately whereas CoA message modifies the user session authorization attributes.

Figure 3 illustrates a CoA message exchange between an 802.1X-enabled client, a switch operating as Authenticator (DAS), and a RADIUS server operating as an Authentication Server (DAC).

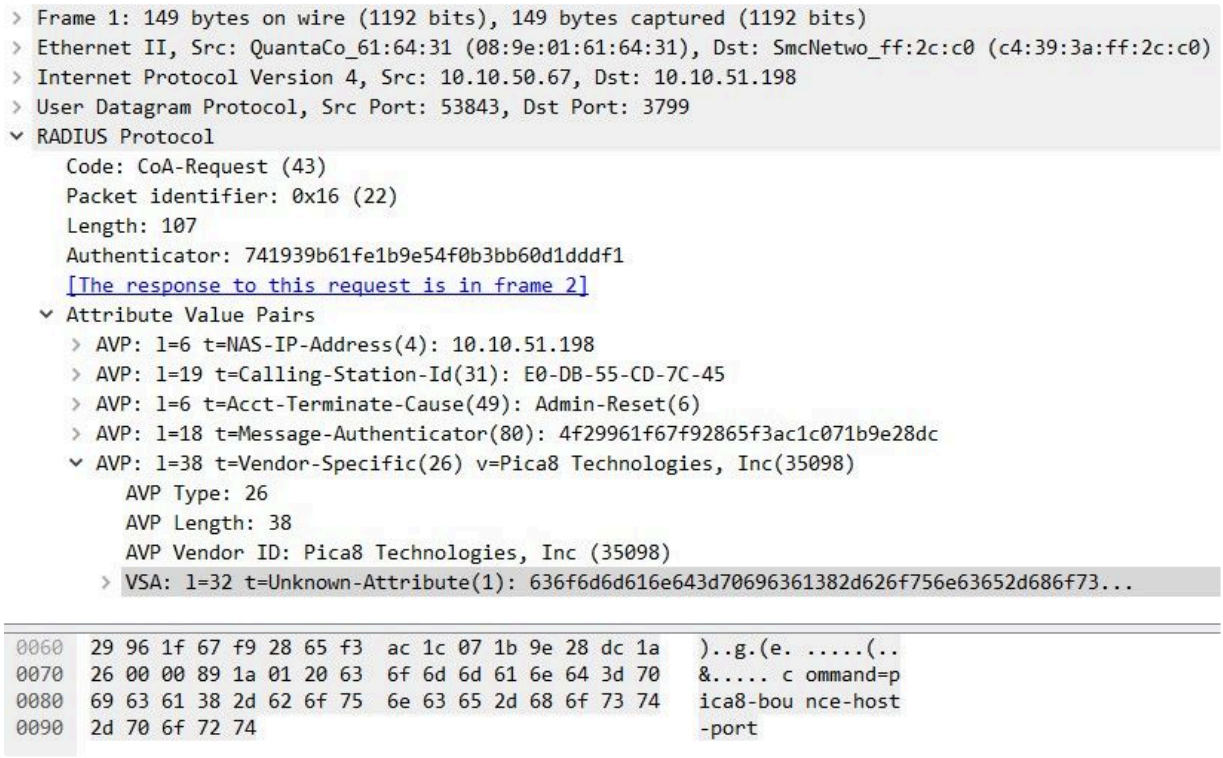
Figure 3. Message Exchange during CoA Process



The AAA server sends a CoA-Request packet to the switch to request to change the user authorization attribute. The packet may include one of the four authorization attributes supported by PICOS: Disconnect, Re-authenticate, Bounce-host-port and Disable-host-port, as shown in Figure 3.

- **Disconnect**: When the switch receives the Disconnect message, it terminates the user session immediately.
- **Re-authenticate**: When the switch receives the re-authenticate CoA Request message from the AAA server, the switch sends an EAP Request message to the supplicant to initiate re-authentication.
- **Bounce-host-port**: The CoA-Request message with bounce-host-port attribute brings the interface down and then up immediately.
- **Disable-host-port**: The CoA-Request message with disable-host-port attribute brings the interface down. The interface cannot be used after this operation. If you want to enable this interface, use the **set interface gigabit-ethernet**<*port*> **disable false** CLI command.

Figure 4. Bounce-host-port Attribute in CoA-Request Message



1. DAS performs the action according to the authorization attribute in the CoA-Request packet.

2. DAS replies with a CoA-ACK/NAK message. While sending the CoA-ACK/NAK, the source port in the CoA-Request packet is used as the destination port whereas the destination port of 3799 in the CoA-Request packet is used as the source port.

- If DAS successfully applies the action in the CoA Request packet it will reply with a CoA-ACK message. DAS replies with a CoA-ACK message.
- If for some reason the DAS is unable to carry out the action requested in the CoA Request packet, the DAS replies with a CoA-NAK message.

Downloadable ACL

The downloadable ACL is a dynamic packet filtering function that is implemented by the AAA server and the firewall filter module of the switch. To use downloadable ACL, users have to configure the ACL name and the detailed ACL rules on the AAA server; the switch only has to enable 802.1X authentication or MAB authentication locally.

After the 802.1X authentication or MAB authentication has succeeded, the AAA server sends the ACL to the switch in the Access-Accept message. The switch parses the received downloadable ACL field and implements packet filtering through the packet matching rules and processing operations. The downloadable ACL is delivered to a specific MAB or 802.1X user and is delivered only when the respective authentications are passed successfully.

For downloadable ACL, PICA8 has defined two vendor-specific-attributes (VSAs) on the AAA server. First one is the **Pica8-IP-Downloadable-ACL-Name**, the attribute ID number is 3, and **Pica8-IP-Downloadable-ACL-Rule**, the attribute ID number is 2 in the PICA8 RADIUS dictionary. To use these VSAs the users have to import the PICA8 RADIUS dictionary to the AAA server. For details about how to import PICA8 RADIUS dictionary, please refer to the document How to Import PICA8 RADIUS Dictionary.

The values for **Pica8-IP-Downloadable-ACL-Rule** attribute are implemented based on the firewall filter module. The template of supported matching conditions/actions are as follows.

Template of Downloadable ACL:

```
sequence [0..9999] from destination-address-ipv4 <IPv4Net>
```

sequence [0..9999] from source-address-ipv4 <IPv4Net>

sequence [0..9999] from destination-address-ipv6 <IPv6Net>

sequence [0..9999] from source-address-ipv6 <IPv6Net>

sequence [0..9999] from destination-port <uintrange>

sequence [0..9999] from source-port <uintrange>

sequence [0..9999] from ether-type [1501..65535]

sequence [0..9999] from protocol icmp

sequence [0..9999] from protocol icmp [type|code] [0..254]

sequence [0..9999] from protocol igmp

sequence [0..9999] from protocol ip

sequence [0..9999] from protocol tcp

sequence [0..9999] from protocol ospf

sequence [0..9999] from protocol others [0..255]

sequence [0..9999] then action [discard|forward]

and is the logical operator between the matching fields with the same sequence number, that is, to be considered to match a firewall filter rule and included in a class, the packets must match all of the matching fields with the same sequence number. NOTE that there is a drop rule for each firewall filter rule by default.

To reduce the size of Access-Accept message, PICOS supports parsing the abbreviation downloadable ACLs. The following table shows the supported abbreviation styles.

Full keywords	Abbreviation
sequence	s, se, seq
destination-address-ipv4	dip4
destination-address-ipv6	dip6
destination-port	dp, dport
source-address-ipv4	sip4
source-address-ipv6	sip6
source-port	sp, sport
protocol	pro
then	t, th
from	f, fr
action	a, ac, act
discard	di, dis, disc
forward	fo, for, forw
ether-type	etyp

It is also supported to merge multiple **from** statements and **action** statements of the same sequence number into one single line.

For example,

For the following downloadable ACL rules.

```
sequence 100 from protocol tcp
sequence 100 from source-port 443
sequence 100 from destination-address-ipv4 63.18.0.0/16
sequence 100 then action forward
```

The equivalent ACL rule to that is:

```
sequence 100 from protocol tcp from source-port 443 from destination-address-ipv4 63.18.0.0/16 then action forward
```

or

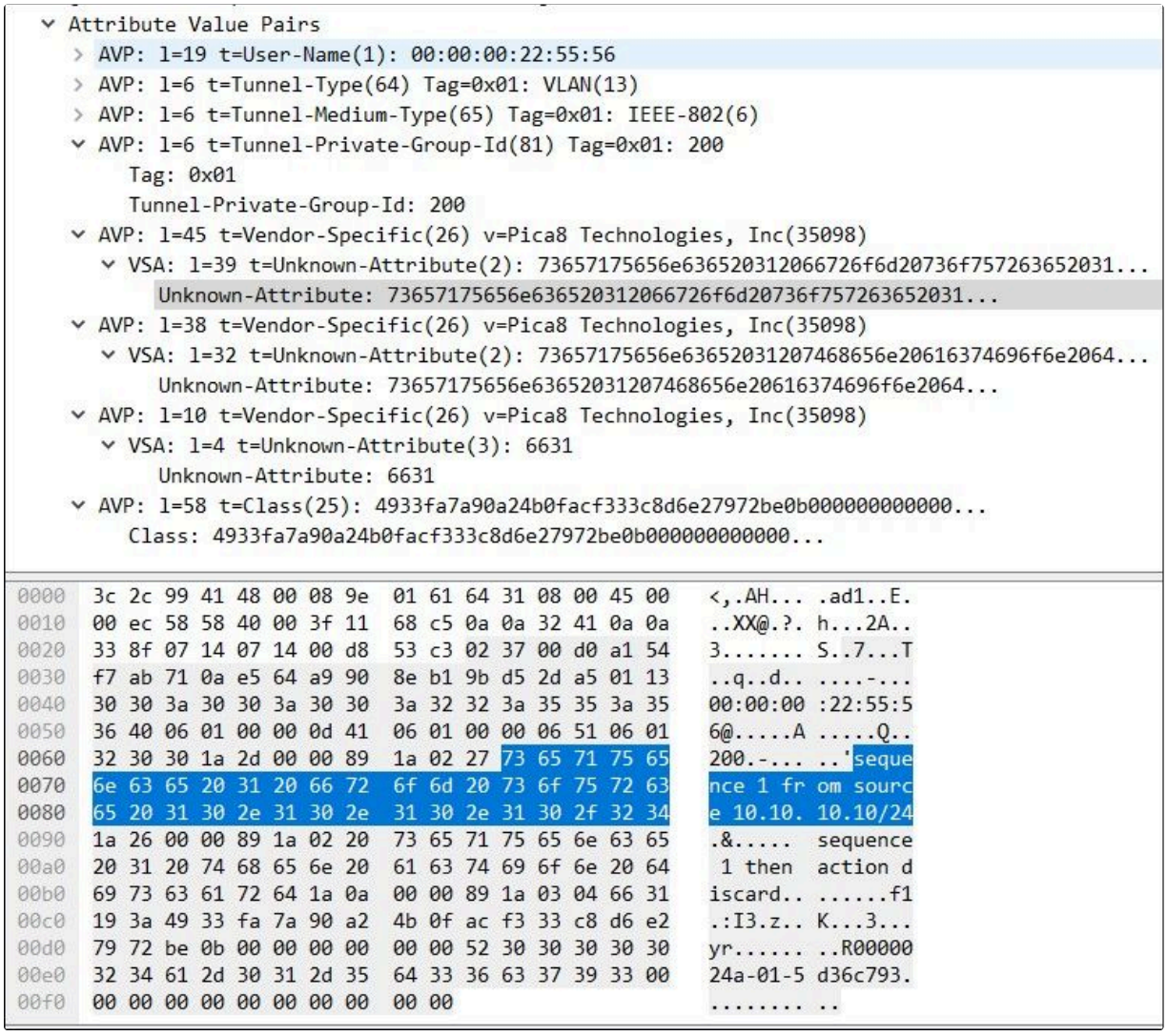
```
s 100 f pro tcp f sp 443 f dip4 63.18.0.0/16 t a fo
```

This equivalent ACL greatly reduces the size of the Access-Accept message.

NOTE:

- If the format or the content of the downloadable ACL do not meet the template conditions mentioned above, the ACL rule fails to be parsed and applied to the hardware.
- On the AAA server, make sure you use only one Pica8-IP-Downloadable-ACL-Name attribute which carries the downloadable ACL name, but you can have multiple Pica8-IP-Downloadable-ACL-Rule attributes.

The following image shows the format of the downloadable ACL in the Access-Accept message which is sent from the AAA server to the switch:



On the switch, you can use the **run show dot1x interface** and **run show dot1x downloadable filter** commands to view the detailed information about the downloadable ACL delivered by the interface.

For example,

```
admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/48
Interface ge-1/1/48:
============================================================
Client MAC                              : 00:00:00:11:11:11
Status                                      : authorized
Success Auth Method             : MAB
Last Success Time                   : Sun Mar 20 21:08:11 2022
Traffic Class                             : Other
Downloadable Filter Name     : pica-dacl-mab (active)
============================================================


admin@Xorplus# run show dot1x downloadable filter
=============================================
Filter: pica-dacl-mab
Description     :
---------------------------------------------------------------------
Sequence        : 1
Description     :
Match counter   : 0 packets
```

```
Match Condition : L4 Destination Port  : 67..67
                  L4 Source Port       : 68..68
                  Protocol             : udp
                  Action               : Forward
```

The employment of the downloadable ACL and the configuration examples on the ClearPass/Cisco ISE and the switch are detailed in the document Configuring Dynamic and Downloadable ACL for ClearPass and Configuring Dynamic and Downloadable ACL on Cisco ISE in Typical Configuration of NAC.

NOTE:

- PICOS supports configuring ACL rules based on firewall filter for ports on which dynamic/downloadable ACLs of NAC are already configured. If both types of ACL rules are configured, the matching rules are as follows:

  The priority of the firewall filter-based ACL rule is higher than that of the NAC dynamic/downloadable ACL. However, in the case when the message hits an ACL rule of discard action, the discard rule has the highest priority, that is to say, the message will be discarded, regardless of whether the rule is a firewall filter-based ACL rule or the dynamic/downloadable ACL of NAC.

- When matching ACL rules, the system processes IPv6 rules (**destination-address-ipv6/source-address-ipv6**) with higher priority than other ACL rules. Even if the sequence number of IPv6 rule is larger than the other rules', the IPv6 rule will be processed first.
  For example, confider the ACL rules shown below. The **destination-address-ipv6** rule will be processed first then all the other rules will be processed.

  admin@XorPlus# set dot1x filter MyFilter sequence 100 from source-port 332
  admin@XorPlus# set dot1x filter MyFilter sequence 100 then action discard
  admin@XorPlus# set dot1x filter MyFilter sequence 200 from destination-address-ipv6 2001::1/128
  admin@XorPlus# set dot1x filter MyFilter sequence 200 then action forward

  Therefore, when planning ACL rules, it is recommended to configure IPv6 source/destination rules with smaller sequence numbers. If not then it is highly stressed to keep this exception in mind while trying to achieve the desired effect.

- IPv6 ACL rules cannot be configured with the following rules at the same time:
  - Configuration with ether-type or destination-port is not supported on the ingress port.
  - Configuration with ether-type is not supported on the egress port.

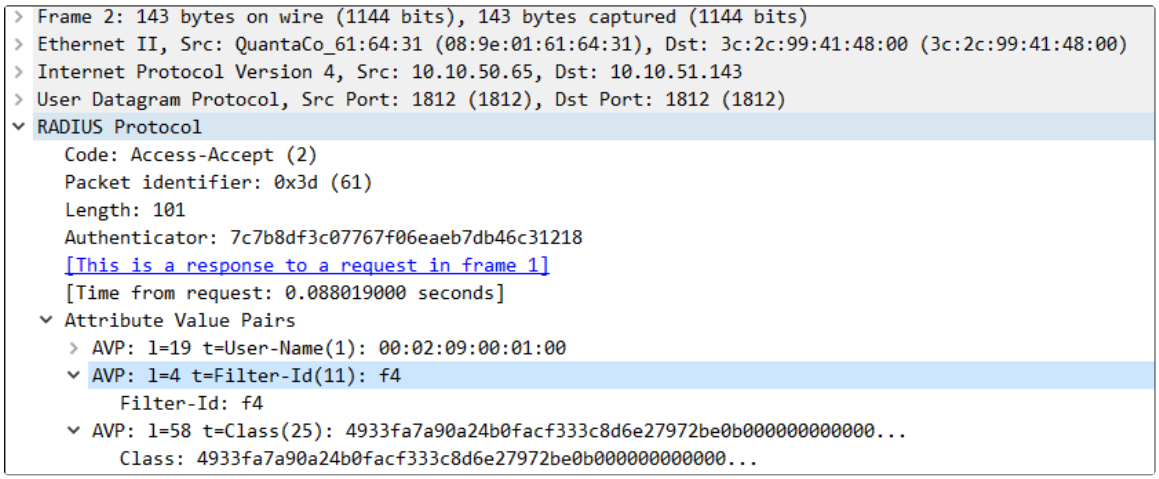
Dynamic ACL

The dynamic ACL is a dynamic packet filtering function that is implemented by the AAA server and the firewall filter module of the switch function. Instead of downloadable ACL getting the detailed ACL rules from the AAA server, the detailed rules of dynamic ACL should be preconfigured on the switch and the ACL should be applied just when the ACL name is received from AAA server. The name of the dynamic ACL is configured on the AAA server which uses the RADIUS standard attribute **Filter-Id**, an attribute defined by the RFC3576 standard and the attribute ID number is 11.

After the 802.1X authentication or MAB authentication has succeeded, the AAA server sends the ACL name to the switch in the Access-Accept message carried with Filter-Id field. The switch parses the received dynamic ACL field and implements packet filtering through the packet matching rules and processing operations. Each dynamic ACL is sent only with an Access-Accept message when any of MAB or 802.1X authentication has passed successfully on the AAA server for a specific client.

The switch delivers the ACL rule to match the packets and process the packets to implement packet filter rule. If the AAA server delivers a wrong ACL name, the switch prints a system log, and then drops the flow by using the default drop rule.

The following image shows the format of Filter-ID in the Access-Accept message which is sent from the AAA server to the switch:



On the switch, use the following commands to configure the NAC-based dynamic ACL rule.

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from** <*filter-condition*>

set protocols dot1x filter <*filter-name*> **sequence** <*number*> **then action** <**discard** | **forward**>

and is the logical operator between the matching fields with the same sequence number, that is, to be considered to match a firewall filter rule and included in a class, the packets must match all of the matching fields with the same sequence number. NOTE that there is a drop rule for each firewall filter rule by default.

On the switch, you can use the **run show dot1x interface** command to view the detailed information about the dynamic ACL applied to the interface.

For example,

admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/5

Interface ge-1/1/5:

==========

Client MAC : 08:9e:01:9e:cc:fe

Status : authorized

Dynamic VLAN ID : 200

Dynamic Filter Name : f2

The employment of the dynamic ACL and the configuration examples on the ClearPass/Cisco ISE and the switch are detailed in the document Configuring Dynamic and Downloadable ACL for ClearPass and Configuring Dynamic and Downloadable ACL on Cisco ISE in Typical Configuration of NAC.

NOTE:

- The filter name configured in the filter-id must be the same as the filter name of the dynamic ACL configured on the switch.
- PICOS supports configuring ACL rules based on firewall filter for ports on which dynamic/downloadable ACLs of NAC are already configured. If both types of ACL rules are configured, the matching rules are as follows:

  The priority of the firewall filter-based ACL rule is higher than that of the NAC dynamic/downloadable ACL. However, in the case when the message hits an ACL rule of discard action, the discard rule has the highest priority, that is to say, the message will be discarded, regardless of whether the rule is a firewall filter-based ACL rule or the dynamic/downloadable ACL of NAC.

Response to session-timeout Attribute

If the returned access-accept RADIUS message carries the attribute session-timeout after MAB/802.1X authentication, the authenticated session will expire after a period of session-timeout and start a new authentication process.

- If the access-accept RADIUS message carried the timeout-session attribute and the timeout value is not equal to 0 (such as 30s), the switch will send request packet to the AAA server or the client every 30s for re-authentication.
- If the access-accept RADIUS message carried the timeout-session attribute but the timeout value is equal to 0, the switch does not send any re-authentication request packet to the AAA server or the client. No action is taken, it has the same effect as if the session timeout attribute was not used or the returned access accept packet did not had the timeout attribute.
- If the access-accept RADIUS message does not include the timeout-session attribute, the switch will send the re-authentication request packet to the AAA server or the client every 60 mins (default value) for re-authentication. The default 60 minutes re-authentication applies in situations where the MAC address does not age out for 60 minutes.

Vendor Specific Attribute (VSA)

Vendor Specific Attribute (VSA) is a vendor defined attribute in the vendor's RADIUS dictionary. For the NAC function, PICOS defines four VSAs whereas the PICA8 vendor ID is 35098:

Pica8-AVPair, the attribute ID number is 1;

Pica8-IP-Downloadable-ACL-Rule, the attribute ID number is 2;

Pica8-IP-Downloadable-ACL-Name, the attribute ID number is 3;

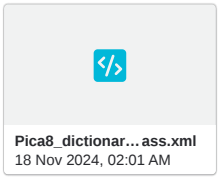
Pica8-Redirect-URL, the attribute ID number is 4.

To use these VSAs, the users have to import the PICA8 RADIUS dictionary to AAA server. We describe how to import PICA8 RADIUS dictionary to ClearPass, Cisco ISE and FreeRadius below.

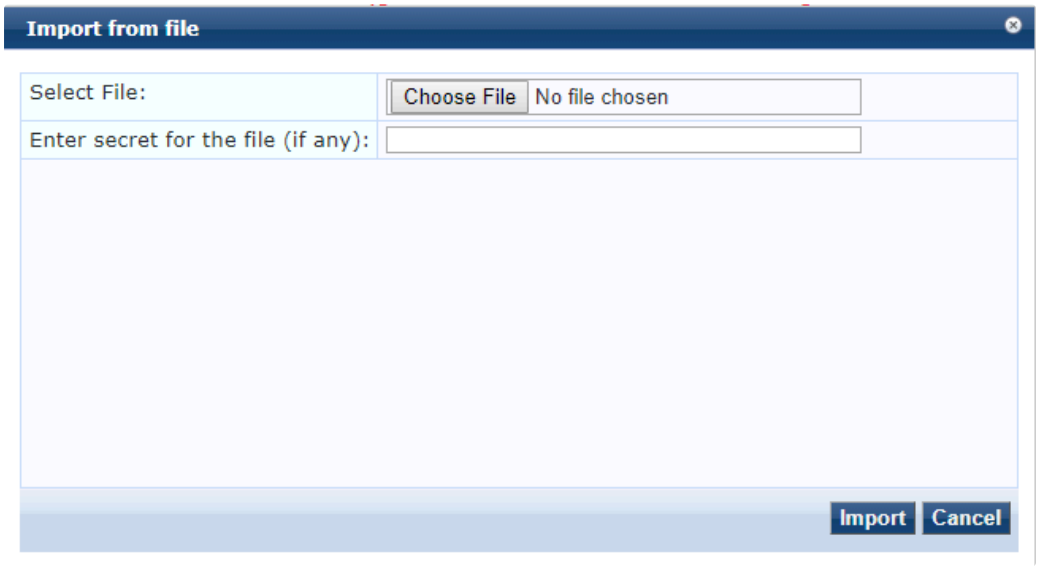
How to Import PICA8 RADIUS Dictionary to ClearPass

To import the PICA8 RADIUS dictionary file to ClearPass, perform the following tasks in CPPM on ClearPass.

1. Click on **AdministrationàDictionariesà**
2. Click on **Import** (top right corner).
3. Choose the PICA8 RADIUS dictionary file and click **Import**.
4. You can use the PICA8 RADIUS dictionary file attached below if you don't have it.



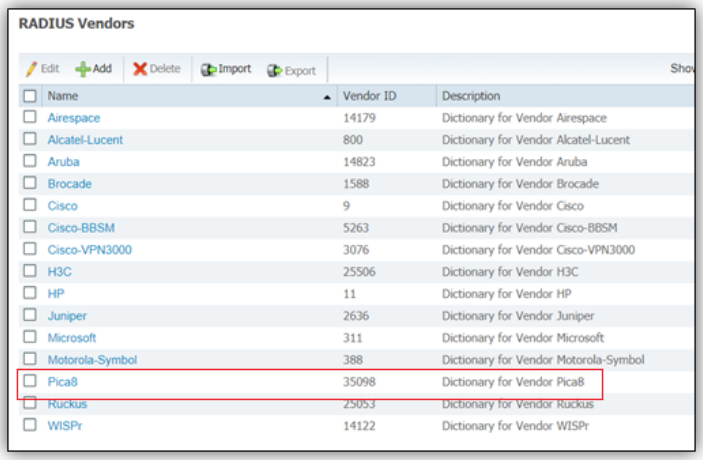
5. Refer to the image below for reference.

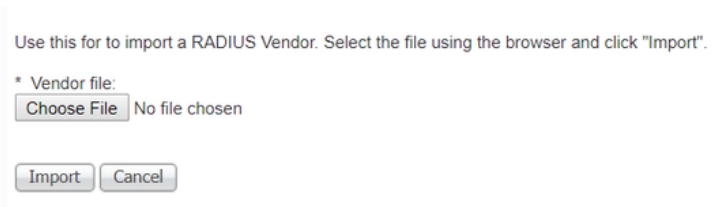


How to Import PICA8 RADIUS Dictionary for Cisco ISE

We need to import the Pica8 radius dictionary file to ISE for Pica8 switches to work properly with ISE. Follow the steps below to import the dictionary file.

1. Click on **Policy Elements -> Dictionaries -> System -> Radius -> RADIUS Vendors**.
2. Click on Import and choose the Pica8 dictionary file, now click import to load the dictionary file.
3. You should be able to see Pica8 dictionary file in the list of vendor dictionaries after successful import.



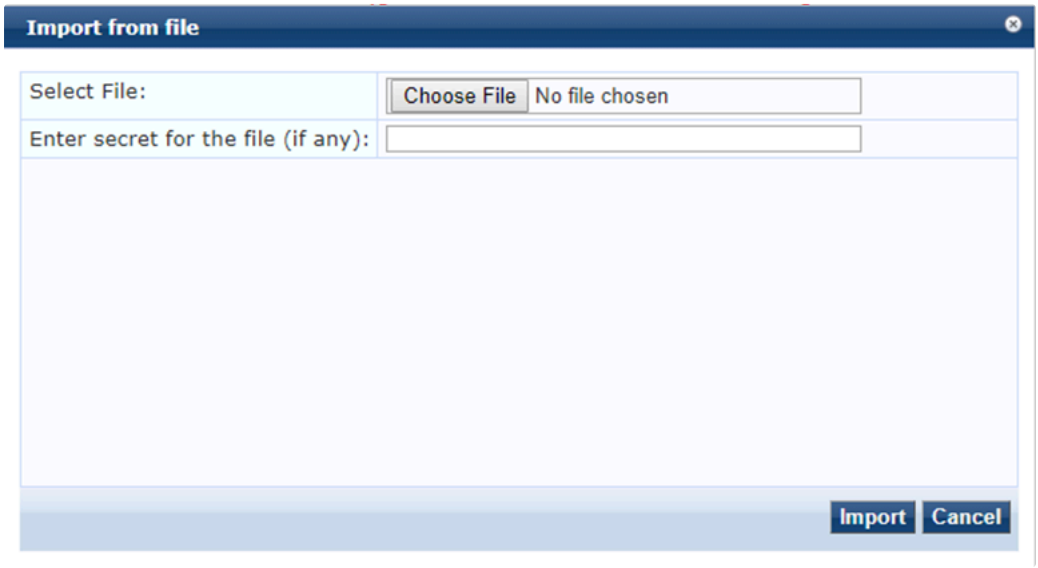


4. You can also create your dictionary file here by clicking Add and adding attributes as mentioned in dictionary file.
5. Please note adding a dictionary file manually you need to enter the attributes as they are in the dictionary files. The two most important items are the VENDOR name and ID and Pica8-AVPair attribute. The VENDOR name must be set to Pica8 and the ID should be 35098.
6. The dictionary file for Cisco ISE is attached below:



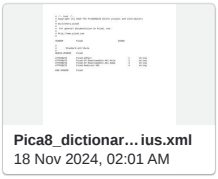
Pica8_dictionary_ISE.xml
18 Nov 2024, 02:01 AM

7. Refer to the image below for reference.



How to Import PICA8 RADIUS Dictionary to FreeRadius server

To import the Pica8 Radius dictionary to FreeRadius server, copy the file attached below to location ***/usr/share/freeradius/***.



Pica8_dictionar… ius.xml
18 Nov 2024, 02:01 AM

Configuring NTP and the Time Zone Parameter

> **NOTE:**
> NTP does support IPv6.

Configuring the NTP Server IP Address

The L2/L3 switch synchronizes with the NTP server only when the configuration commands are committed using the **commit** command. User can change the NTP server's IP address, as shown below.

```
admin@XorPlus# set system ntp server-ip 192.168.10.100
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the NTP Source Interface

NTP source interface is required if inband management interface is used to connect with the NTP server. Note that if the NTP source interface is not configured, the system will print an error log.

```
admin@XorPlus# set system ntp source-interface vlan-300
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the Time Zone

Configure the time zone as follows (The time zone configured below is Pacific/Kosrae).

```
admin@XorPlus# set system timezone Pacific/Kosrae
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the System Clock

```
admin@XorPlus> set date 2012.01.01-23:59
Sun Jan 1 23:59:00 UTC 2012
admin@XorPlus>
```

The clock will be set in the hardware.

Configuring PTP

- Principle
  - Introduction to PTP
  - Basic Concepts
  - Delay Request-Response Mechanism
- Product Support
- PTP Configuration
  - Procedure
- Configuration Example

Principle

> The PicOS supports PTP function since 2.9.2.

Introduction to PTP

On a modern communication network, most telecommunications services require that the frequency offset or time difference between devices is within an acceptable range. To meet this requirement, network clock synchronization must be implemented.

Network clock synchronization includes phase synchronization and frequency synchronization.

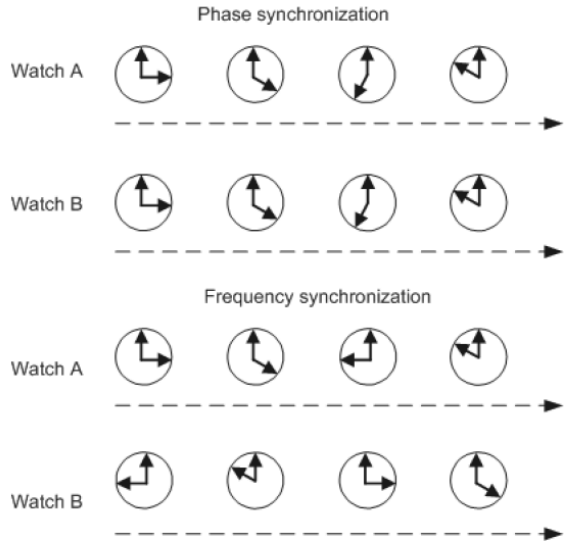
Phase synchronization

Phase synchronization, also called time synchronization, refers to the consistency of both frequencies and phases between signals. That is to say, the phase difference between signals is always 0.

Frequency synchronization

Frequency synchronization refers to constant phase difference between signals. It ensures that signals are sent or received at the same rate at a moment so that all devices on the communication network operate at the same rate.

Figure 1 Difference between phase synchronization and frequency synchronization



PTP (Precision Time Protocol) is a time synchronization protocol, which is not only used for high-precision time synchronization between devices, but can also be used to synchronize the frequency between devices. Compared to the existing time synchronization mechanism, PTP has the following advantages:

- Compared to NTP (Network Time Protocol), PTP can meet the more accurate time synchronization requirements, NTP generally can only achieve sub-second time synchronization accuracy, and PTP can reach sub-microsecond.
- Compared to GPS (Global Positioning System), PTP has lower construction and maintenance costs, and because it can get rid of the dependence on GPS, it has special meaning in national security.

Basic Concepts

PTP domain

A PTP domain is a logical grouping of clocks that synchronize to each other using the protocol IEEE 1588v2, but that are not necessarily synchronized to clocks in another domain. Each PTP domain is an independent PTP clock synchronization system and has only one clock source.

Clock node

Clock nodes are nodes in a PTP domain. PTP defines the following types of clock nodes:

- Ordinary clock (OC) device: provides only one physical port to participate in time synchronization in a PTP domain. An OC device uses this port to synchronize time with an upstream device or send time to a downstream device.

- Boundary clock (BC) device: provides two or more physical ports to participate in time synchronization in a PTP domain. One port synchronizes time with an upstream device, and the others send the time to downstream devices. A clock node is also a BC device if it functions as the clock source and sends time to downstream devices through multiple PTP ports.
- Transparent clock (TC) device: forwards PTP messages between its PTP ports and measures the link delay of the messages. Different from an OC device and a BC device, a TC device does not synchronize time with other devices through ports.
    - E2ETC (End-to-End Transparent Clock): forwards packets of non-P2P (non-Peer-to-Peer) types directly on the network and participates in the calculation of the entire link Time.

      E2ETC calculate the residence time of the device, which is the time it takes the event message from ingress port to egress port, then add the calculated residence time to the correctionfield of the event message.

    - P2PTC (Peer-to-Peer Transparent Clock): forwards only Sync messages, Follow_Up messages and Announce messages, and terminates other PTP packets, and participates in the calculation the delay of each link on the entire link.

PTP port

A PTP port is a port running PTP. PTP ports are classified into the following types based on roles:

- Master port: The port is the source of time on the path served by the port, located on a BC or OC device.
- Slave port: The port synchronizes to the device on the path with the port that is in the MASTER state, located on a BC or OC device.
- Passive port: The port is not the master on the path nor does it synchronize to a master. It is an idle port on a BC device and does not receive or send synchronization clock signals.

Master-slave hierarchy

Nodes in a PTP domain establish the master-slave hierarchy for clock synchronization. Master nodes send synchronization clock signals, while slave nodes receive synchronization clock signals. A device may receive synchronization clock signals from an upstream node and then send the synchronization clock signals to a downstream device.
If two clock nodes synchronize time with each other:

- The node that sends synchronization clock signals is the master node, and the node that receives synchronization clock signals is the slave node.
- The clock on the master node is the master clock, and the clock on the slave node is the slave clock.
- The port that sends synchronization clock signals is the master port, and the port that receives synchronization clock signals is the slave port.

Grandmaster clock

All clock nodes in a PTP domain are organized into the master-slave hierarchy. The grandmaster clock (GMC) is at the top of the hierarchy and is the reference clock in the PTP domain. Clock nodes exchange PTP messages to synchronize the time of the GMC to the entire PTP domain. Therefore, the GMC is also called the clock source. The GMC can be statically configured or dynamically elected through the best master clock (BMC) algorithm.

PTP message

Nodes exchange PTP messages to establish the master-slave hierarchy and implement time and frequency synchronization. PTP messages are classified into event messages and general messages depending on timestamps:

- Event message: is tagged with a timestamp when reaching or leaving a port. PTP devices calculate the link delay based on the timestamps carried in event messages. Event messages include Sync, Delay_Req, Pdelay_Req, and Pdelay_Resp messages.
- General message: is used to establish master-slave hierarchy, and to request and send time information. General messages are not tagged with timestamps. General messages include Announce, Follow_Up, Delay_Resp, Pdelay_Resp_Follow_Up, Management, and Signaling messages.

> **NOTE：**
> Currently, devices support only E2ETC function, and uses Sync, Delay_Req and Delay_Resp PTP messages.

Delay Request-Response Mechanism

Figure 2 shows the process of calculating the average link delay and time offset between the master and slave devices using the E2E mechanism.

Figure 2 Delay request-response mechanism

1. The master sends a Sync message to the slave and notes the time t1 at which it was sent.
2. The slave receives the Sync message and notes the time of reception t2.
3. The master conveys to the slave the timestamp t1 by:
   a) Embedding the timestamp t1 in the Sync message. This requires some sort of hardware processing for highest accuracy and precision.
   b) Embedding the timestamp t1 in a Follow_Up message.
4. The slave sends a Delay_Req message to the master and notes the time t3 at which it was sent.
5. The master receives the Delay_Req message and notes the time of reception t4.

The master conveys to the slave the timestamp t4 by embedding it in a Delay_Resp message.
By exchanging messages with the master device, the slave device obtains t1, t2, t3, and t4, and calculates the average link delay and time offset between the master and slave devices. Then the slave device can adjust the local time according to the calculated time offset to synchronize with the master device. The formulas for calculating the link delay and time offset are as follows:

Average link delay = [(t4- t1) - (t3- t2)]/2
Offset = [(t2- t1) + (t3- t4)]/2

Product Support

The table below shows the model and the corresponding switch ASIC that support the PTP function, others do not support.

Switch ASIC	Model
Trident3	AS7726-32X
	AS7326-56X
	AS5835-54T
	AS5835-54X
	AS4630-54NPE
	AS4630-54PE
	S5232F-ON
	S5296F-ON
	S5248F-ON
	S5224F-ON
	S5212F-ON
	N3248P-ON
	N3248TE-ON
	N3224P-ON
	N3224T-ON
	N3224F-ON
	N3248PXE-ON
	N3224PX-ON
	N3248X-ON
Helix4	as4610-30t
	as4610_30p
	as4610_54t
	as4610_54p
Trident2	pronto5101
	pronto5401
	as6701-32x
	as6712-32x
	pronto5101
	as5712-54x
	s4048
	arctica4806xp
Trident2Plus	as5812-54t
	as5812-54x
Tomahawk	dcs7032q28
	z9100
	as7312
	as7712-32x

PTP Configuration

Configure the device interface as the E2ETC node type, enable the PTP function on the interface, and implement the device to forward the PTP packets directly.

Procedure

Step 1. Configure the device interface as the E2ETC node type, enable the PTP function on the interface.

set interface gigabit-ethernet <*port*> **ptp mode** {e2etransparent | none}

By default, PTP is disabled on an interface.

NOTE :

- The PTP function can only be configured on the physical interface.
- On the TC device, PTP must be enabled on all the interfaces that receive and send PTP messages. Otherwise, the PTP function will work inproperly.

Configuration Example

Procedure

Step 1. Configure the port te-1/1/25 that receiving PTP messages and the port te-1/1/26 that sends PTP packets as E2ETC node.

admin@Xorplus#set interface gigabit-ethernet te-1/1/25 ptp mode e2etransparent

admin@Xorplus#set interface gigabit-ethernet te-1/1/26 ptp mode e2etransparent

Step 2. Verify the configuration.

After the configuration is complete, run the **run show interface detail** command to view the configuration of PTP.

```
admin@Xorplus# run show interface gigabit-ethernet te-1/1/25 detail
Physical interface: te-1/1/25, Enabled, error-discard False, Physical link is Down
Interface index: 25, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:0, egress:0
Precision Time Protocol mode:e2etransparent
Current address: 48:6e:73:01:00:61, Hardware address: 48:6e:73:01:00:61
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
  -More-
```

Configuring the linux-config-unreliable

PicOS is a Linux distribution with Pica8 tools for Routing, Switching, and OpenFlow. As such, PicOS can be configured directly from the Linux shell.

But sometimes, operators would like to be sure the CLI configuration completely reflects the state of the system. It can be useful if the same parameter can be configured in the CLI, or in Linux at the same time. A good example of such parameters would be the IP address of the system or its default gateway.

In the PicOS CLI configuration, all of those parameters have been gathered under the system hierarchy. It is then the choice of the operator to choose either the CLI or Linux shell to configure the system parameters.

A new knob has been added for control, in case the CLI configuration should override the Linux configuration.

By default, the CLI configuration does NOT override the Linux system configuration.

> When the linux-config-unreliable knob is modified, please commit it first, then set other system settings.
> Do not commit the linux-config-unreliable and system delta at the same time.

You can choose bash control or xorp control. As shown below:

Xorp Control

```
admin@XorPlus# set system linux-config-unreliable true
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# show system
    linux-config-unreliable: true
    }
    log-level: "trace"
```

Bash Control

```
admin@XorPlus# set system linux-config-unreliable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# show system
    linux-config-unreliable: false
    log-level: "trace"
```

If user chooses bash control, the system settings should be set in bash, not from xorp. Otherwise, the system command should be set in xorp.

```
admin@XorPlus# show system
    linux-config-unreliable: false
    log-level: "trace"
admin@XorPlus# set system hostname pica8
admin@XorPlus# commit
The system is managed by linux
Commit failed.
admin@XorPlus#
```

> The following system commands should always be set in PicOS, even when system is under bash control:
>
> system aaa tacacs-plus
>
> system log-level
>
> > When changing the system control straight from xorp control to bash control, the xorp configurations related to system will be removed from the configuration tree automatically. When changing from Bash control to xorp control, the configuration related to the system will be read and added into the xorp configuration tree automatically.
>
> system log-facility

Configuring IPFIX

Configuring IPFIX Parameters

By default, IPFIX is disabled. You can enable IPFIX and configure its parameters, as shown below. Make sure the switch can connect to the IPFIX collector server correctly.

```
admin@XorPlus# set protocols ipfix collector 192.168.2.10 udp-port 9999
admin@XorPlus# set protocols ipfix interfaces ingress ge-1/1/1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring sFlow

NOTEs:

- User needs to enable sFlow on global and on the port so that it can sample flow and counters. If sFlow is only enabled on global, it will only see the port count.
- The following sampling field of sFlow nexthop IP in sFlow version5 Extended Router Data is supported.

```
/* Extended Router Data */
/* opaque = flow_data; enterprise = 0; format = 1002 */
struct extended_router {
   next_hop nexthop;            /* IP address of next hop router */
   unsigned int src_mask_len;   /* Source address prefix mask
                                   (expressed as number of bits) */
   unsigned int dst_mask_len;   /* Destination address prefix mask
                                   (expressed as number of bits) */
}
```

- For packets forwarded via ECMP routes, sFlow selects nexthop of one of the ECMP routes as the nexthop information of the packet in the sampling information, which may not necessarily be the nexthop of the route used for actual packet forwarding.

Globally Enabling sFlow

By default, sFlow is disabled. User can enable sFlow and configure the parameters, verify that the switch can connect to the sFlow collector server, and configure the sFlow **agent-id** and **source-address** at the same time that sFlow is enabled.

```
admin@XorPlus# set protocols sflow disable false
admin@XorPlus# set protocols sflow agent-id 10.10.50.248
admin@XorPlus# set protocols sflow source-address 10.10.50.248
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring sFlow Parameters

User can configure global parameters for sFlow, including agent-id, collector IP, polling-interval, sampling-rate, and source-address.

```
admin@XorPlus# set protocols sflow agent-id 10.10.50.248
admin@XorPlus# set protocols sflow collector 10.10.50.221 udp-port 6343
admin@XorPlus# set protocols sflow polling-interval 30
admin@XorPlus# set protocols sflow sampling-rate ingress 2000
admin@XorPlus# set protocols sflow sampling-rate egress 2000
admin@XorPlus# set protocols sflow header-len 128
admin@XorPlus# set protocols sflow source-address 10.10.50.248
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# run show sflow
sFlow : Enabled
Agent ID : 10.10.50.248
Source Address : 10.10.50.248
Sample rate ingress: 1:2000
Sample rate egress : 1:2000
Polling interval : 30 seconds
Header Length : 128
admin@XorPlus#
admin@XorPlus# run show sflow collector
Collector address UDP-port No of Samples
---------------- -------- -------------
10.10.50.221 6343 5336
```

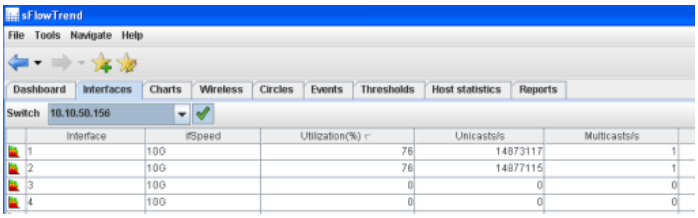
```
admin@XorPlus#
```

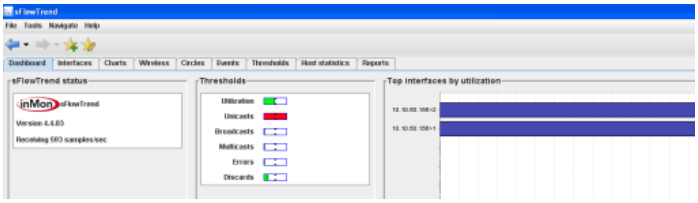
Configuring sFlow on a Specific Interface

User can configure sFlow parameters on a specific interface but needs to enable sflow protocols on global first.

```
admin@XorPlus# set protocols sflow interface ge-1/1/1 ?
Possible completions:
  <[Enter]>                    Execute this command
  disable                      Disable sflow on all interfaces by default
  header-len                   The Length of sampled packet in bytes, 64 by default
  polling-interval             How often the sflow agent polls the interface in seconds, 30 by default
  sampling-rate                The rate at which packets must be sampled, 2000 by default
admin@XorPlus# set protocols sflow interface ge-1/1/1 disable false
admin@XorPlus# set protocols sflow interface ge-1/1/1 header-len 128
admin@XorPlus# set protocols sflow interface ge-1/1/1 polling-interval 10
admin@XorPlus# set protocols sflow interface ge-1/1/1 sampling-rate ingress 1000
admin@XorPlus# commit
```

In the current version, sFlow samples only the ingress traffic of each interface. User can monitor the traffic with sFlow Trend.





Configuring the Syslog Log Level

Configuring the Syslog Level

Our system has five syslog levels. Listed in order of most fatal to least fatal, the levels are: Fatal, Error, Warning, Info, and Trace. By default, the system is set to the Warning level. You can, of course, change the log level by using the command **set system log-level**.

In the example below, the system logs messages from Info, Warning, Error, and Fatal levels since the system syslog level is set to Info.

```
admin@XorPlus# set system log-level info
admin@XorPlus# commit
Commit OK.
Save done.

admin@XorPlus#

// You can display the log messages on the console screen by entering the following command:

admin@XorPlus# exit
admin@XorPlus> syslog monitor on

// If the switch's syslog level is Trace, the trace options of the modules should be turned on, as illustrated belo

admin@XorPlus# set protocols ospf traceoptions packet all detail
admin@XorPlus# set system log-level trace
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# exit
admin@XorPlus> syslog monitor on
```

Configuring the Syslog Logging Facility

In accordance with the syslog standard, the logging facility can be configured as [0, 7].

```
admin@XorPlus# set system log-facility 0
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
Oct 17 15:22:42 XorPlus local0.warn : admin logined the switch
Oct 17 15:22:50 XorPlus local0.warn pica_sh: Tacacs send acct body send failed: wrote -1 of 127: Connection refused
Oct 17 15:22:42 XorPlus local2.warn : admin logined the switch
admin@XorPlus# set system log-facility 2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the Syslog Disk and Syslog Server

> **NOTE:**
> Syslog protocol runs in management VRF by default. If you use Ethernet management interface Eth0/1 to connect with the syslog server, you do not need to do the following operations.
>
> However, if the L3 VLAN interface is used to connect with the syslog server, the syslog protocol cannot run normally by default, as all the L3 VLAN interface is in the default VRF by default. You need to modify the configurations to make the L3 VLAN interface management interface and syslog protocol run in the same VRF, so as to run the syslog protocol normally. You can choose either one of the following two ways:
>
> Way 1. Use the command **set system management-services vrf default** to move syslog protocol to run in the default VRF. This way is recommended. Note that using this command also moves the NTP/TACACS+/RADIUS management services to the default VRF.
>
> Way 2. Use the command **set l3-interface vlan-interface** <*interface-name*> **vrf mgmt-vrf** to move the L3 VLAN interface connected to the syslog Collector to management VRF.

Configuring the Syslog Server

After you configure the syslog server IP address, the log files will be sent to the syslog server.

```
admin@XorPlus# set system syslog server-ip 192.168.1.1 ?
Possible completions:
  <[Enter]>                    Execute this command
  port                         Remote syslog server port
  protocol                     Remote syslog server protocol
  source-interface               Configure an existing network interface, e.g. vlan20, eth0, loopback or routed ir
admin@XorPlus# set system syslog server-ip 192.168.1.1 protocol udp
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

> It is recommended to configure **UDP** protocol as the port protocol.

Configuring Syslog for Local Storage

You can configure syslog messages to be stored in RAM or in a local SD card.

```
XorPlus# set system syslog local-file disk
XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
XorPlus#
XorPlus# set system syslog local-file ram
XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
XorPlus#
```

Displaying System Information

User can display a system's information, including fan, power supply unit, and serial number information.

Displaying the System Fan

```
admin@XorPlus>show system fan
Fan Status:
Fan 1 speed = 12529 RPM, PWM = 79
Fan 2 speed = 12413 RPM, PWM = 79
Fan 3 speed = 12300 RPM, PWM = 79
```

Displaying the System Power Supply Unit

```
admin@XorPlus> show system rpsu
RPSU 1: Powered on
    TEMPERATURE_1 : 35.62 C / 96.12 F
    TEMPERATURE_2 : 43.56 C / 110.41 F
    TEMPERATURE_3 : 50.31 C / 122.56 F
    FAN_SPEED_1   : 10608 RPM
RPSU 2: Not present
```

Displaying the System Serial Number

```
admin@XorPlus> show system serial-number

MotherBoard Serial Number : TW0WYGRVDNT0097I0015

RPSU 1 Serial Number      : N/A
RPSU 2: Not ready
SFP+    te-1/1/49             :
        Vendor Name           : Hisense
        Vendor PartNr         : LTF8502-BC+
        Serial Number         : CN56GMC2S0
        Module Type           : 10G_BASE_SR
        Cable Length          : 300m
SFP     te-1/1/50             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01408
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP     te-1/1/51             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01641
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP+    te-1/1/52             :
        Vendor Name           : 3M
        Vendor PartNr         : 1410-P17-00-3.00
        Serial Number         : Y30B220863
        Module Type           : 10G_BASE_AOC
        Cable Length          : 30m
```

Displaying Additional System Information

```
admin@XorPlus# run show system temperature
Temperature:
    Board       : 46.00 C / 114.80 F
    CPU         : 41.00 C / 105.80 F
    Switch Chip : 42.00 C / 107.60 F


admin@XorPlus# run show system uptime
01:21:33 up 50 min, load average: 0.04, 0.06, 0.07

admin@XorPlus# run show system cpu-usage
CPU usage: 15%

admin@XorPlus# run show system date
Mon Jan 13 18:11:04 UTC 2014


admin@XorPlus# run show system memory-usage
              total        used        free      shared  buff/cache   available
Mem:        3975876      458560     3201488        6264      315828     3293996
Swap:             0           0           0


admin@XorPlus# run show system name
XorPlus


admin@XorPlus# run show system ntp-status
Please start the ntp server first.
NTP Server information:

NTP Server Sync information:
```

```
ntpq: read: Connection refused

admin@XorPlus#
admin@XorPlus# run show system os
Linux PICOS 5.10.23 #3 SMP Thu Jun 9 10:05:11 CST 2022 x86_64 GNU/Linux

admin@XorPlus# run show system processes brief
PID TTY STAT TIME COMMAND
1 ? Ss 0:01 init [2]
2 ? S< 0:00 [kthreadd]
3 ? S< 0:00 [ksoftirqd/0]
4 ? S< 0:00 [watchdog/0]
5 ? S< 0:02 [events/0]
6 ? S< 0:00 [khelper]
48 ? S< 0:00 [kblockd/0]
55 ? S< 0:00 [ata/0]
56 ? S< 0:00 [ata_aux]
58 ? S< 0:00 [kseriod]
99 ? S 0:00 [pdflush]
101 ? S< 0:00 [kswapd0]
147 ? S< 0:00 [aio/0]
156 ? S< 0:00 [nfsiod]
831 ? S< 0:00 [ftld]
853 ? S< 0:00 [rpciod/0]
857 ? S< 0:00 [kjournald]
2222 ? S 0:00 [pdflush]
2356 ? Ss 0:00 /usr/sbin/cron -L 0
2387 ? Ss 0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
2501 ? S 0:03 pica_cardmgr
2503 ? S 0:59 pica_sif
2649 ? S 0:05 pica_lacp
2664 ? Ss 0:00 dhclient -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases eth0
2666 ? Sl 18:06 pica_lcmgr
2672 ? S 0:04 pica_login
3166 ? Sl 0:00 /usr/sbin/rsyslogd -c5
3457 ? S 0:35 pica_mstp
3462 ? S 0:02 xorp_policy
3464 ? Ss 1:03 /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/run/xorp_rtrmgr.pid
3500 tty1 Ss+ 0:00 /sbin/getty 38400 tty1
3507 tty2 Ss+ 0:00 /sbin/getty 38400 tty2
3508 tty3 Ss+ 0:00 /sbin/getty 38400 tty3
3761 ttyS0 Ss+ 0:00 /sbin/getty -s -L ttyS0 115200 ansi
4050 ? S 0:57 ovs-vswitchd
4422 ? Ss 0:00 in.telnetd: 10.10.50.16
4423 pts/0 Ss 0:00 login -h 10.10.50.16 -p
4424 pts/0 S+ 0:00 -bash
4434 pts/0 S+ 0:03 /pica/bin/pica_sh
6451 ? Ss 0:00 in.telnetd: 10.10.50.18
6452 pts/1 Ss 0:00 login -h 10.10.50.18 -p
6460 pts/1 S+ 0:00 -bash
6469 pts/1 R+ 0:03 /pica/bin/pica_sh
15113 pts/1 R 0:00 ps a
admin@XorPlus# run show system rollback ?
Possible completions:
compare Show the difference between tow rolled back configurations
file Show rolled back configuration file
list Show rolled back file list
admin@XorPlus# run show system rollback compare to 02
3c3
< /Last commit : Mon Jan 13 14:13:01 2014 by admin/
—
> /Last commit : Mon Jan 13 14:11:54 2014 by admin/
83,86d82
< crossflow {
< enable: true
< local-control: true
< }
95,98d90
< crossflow {
< enable: true
< local-control: true
< }
510,514d501
< controller 1 {
< protocol: "tcp"
< address: 10.10.50.47
< port: 6633
< }



admin@XorPlus#
admin@XorPlus# run show system rollback file 02
/XORP Configuration File, v1.0/
/Last commit : Mon Jan 13 14:11:54 2014 by admin/
/PicOS Version : 4.2.3/
/Version Checksum: 24226776f6bc5622030e3b7959d612bf/
interface {
ecmp {
max-path: 4
hash-mapping {
field {
ingress-interface {
disable: true
}
vlan {
disable: true
}
ip-protocol {
disable: true
}
ip-source {
disable: false
}
ip-destination {
disable: false
}
port-source {
disable: false
}
port-destination {
disable: false
}
}
}
```

```
}
aggregate-balancing {
.................................................................


admin@XorPlus# run show system rollback list
-rw-rw-r-- 1 admin xorp 17189 Jun  9 17:30 /pica/config/pica.conf
-rw-rw-r-- 1 admin xorp 20153 Jun  9 16:15 /pica/config/pica.conf.01
-rw-rw-r-- 1 admin xorp 20099 Jun  9 16:13 /pica/config/pica.conf.02
-rw-rw-r-- 1 root  xorp 20044 Jun  9 15:38 /pica/config/pica.conf.03
-rw-rw-r-- 1 admin xorp 19516 Jun  9 13:29 /pica/config/pica.conf.04
-rw-rw-r-- 1 admin xorp 19117 Jun  9 13:29 /pica/config/pica.conf.05

admin@XorPlus# run show system users
admin pts/0 Jan 13 14:19 (10.10.50.16)
admin pts/1 Jan 13 15:03 (10.10.50.18)


admin@XorPlus#
admin@XorPlus# run show system core-dumps
total 0
admin@XorPlus#


admin@XorPlus# run show system connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode
tcp        0      0 127.0.0.1:42503         0.0.0.0:*               LISTEN      1000       63936
tcp        0      0 127.0.0.1:36071         0.0.0.0:*               LISTEN      0          55151
tcp        0      0 127.0.0.1:39591         0.0.0.0:*               LISTEN      0          49159
tcp        0      0 127.0.0.1:41127         0.0.0.0:*               LISTEN      1000       31265
tcp        0      0 127.0.0.1:43049         0.0.0.0:*               LISTEN      0          56034
tcp        0      0 127.0.0.1:36009         0.0.0.0:*               LISTEN      0          48231
tcp        0      0 127.0.0.1:2601          0.0.0.0:*               LISTEN      110        46959
tcp        0      0 127.0.0.1:46091         0.0.0.0:*               LISTEN      0          49153
tcp        0      0 127.0.0.1:2604          0.0.0.0:*               LISTEN      110        47899


admin@XorPlus#  run show system boot-messages
Up time: 17:32:21

[    0.000000] Linux version 5.10.23 (build@4e2ef096fb34) (gcc (Debian 10.2.1-6) 10.2.1 20210110, GNU ld (GNU Binutils for Debian)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz root=LABEL=PicOS rw fsck.mode=force fsckfix net.ifnames=0 rootfstype=ext4 con
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x008: 'MPX bounds registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x010: 'MPX CSR'
[    0.000000] x86/fpu: xstate_offset[3]:  576, xstate_sizes[3]:   64
[    0.000000] x86/fpu: xstate_offset[4]:  640, xstate_sizes[4]:   64
[    0.000000] x86/fpu: Enabled xstate features 0x1b, context size is 704 bytes, using 'compacted' format.
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009ffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000077555ff] usable
[    0.000000] BIOS-e820: [mem 0x0000000077556000-0x00000000077565ff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000077566000-0x000000007ca5efff] usable
[    0.000000] BIOS-e820: [mem 0x000000007ca5f000-0x000000007cb38fff] reserved
[    0.000000] BIOS-e820: [mem 0x000000007cb39000-0x000000007cc1cfff] usable
[    0.000000] BIOS-e820: [mem 0x000000007cc1d000-0x000000007cf85fff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x000000007cf86000-0x000000007f29cfff] reserved
[    0.000000] BIOS-e820: [mem 0x000000007f29d000-0x000000007f339fff] type 20
[    0.000000] BIOS-e820: [mem 0x000000007f33a000-0x000000007f7fffff] usable
[    0.000000] BIOS-e820: [mem 0x000000007f800000-0x000000007fffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000e0000000-0x00000000efffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fd000000-0x00000000fe7fffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000ff000000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000017fffffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] efi: EFI v2.60 by American Megatrends
[    0.000000] efi: ACPI 2.0=0x7cf1d000 ACPI=0x7cf1d000 TPMFinalLog=0x7cf54000 SMBIOS=0x7f1f1000 SMBIOS 3.0=0x7f1f0000 MEMATTR=0x7b
[    0.000000] SMBIOS 3.0.0 present.
[    0.000000] DMI: Dell EMC N3248PXE-ON/N3248PXE-ON-CPU, BIOS 3.45.0.9-3 10/17/2019
[    0.000000] tsc: Detected 1500.000 MHz processor
[    0.000028] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.000039] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.000059] last_pfn = 0x180000 max_arch_pfn = 0x400000000
[    0.000070] MTRR default type: uncachable
[    0.000073] MTRR fixed ranges enabled:
 --More--
```

IPv6 Management Support

SNMP over IPv6

User can walk the SNMP model via IPv6 address.

SSH over IPv6

User can log in to the switch via IPv6 address. (Static IPv6 address for a management port can be configured.)

```
admin@XorPlus# set system management-ethernet eth0 ip-address ?
Possible completions:
<[Enter]> Execute this command
IPv4 IPv4 address or negotiated via DHCP, e.g. 192.168.1.2/24 or dhcp
IPv6 IPv6 address or negotiated via DHCP, e.g. fec0::10/64 or dhcp
admin@XorPlus# set system management-ethernet eth0 ip-gateway ?
Possible completions:
<[Enter]> Execute this command
IPv4 Configure the IPv4 gateway
IPv6 Configure the IPv6 gateway
```

Syslog over IPv6

User can send syslog via IPv6 address to remote server.

```
admin@XorPlus# set system syslog server-ip ?
Possible completions:
<IPv4> Remove syslog server
<IPv6> Remove syslog server for IPv6
```

NTP Client IPv6

User can synchronize the time via IPv6 address.

```
admin@XorPlus# set system ntp-server-ip ?
Possible completions:
<IPv4> Sync time with NTP server <IP>
<IPv6> Sync time with NTP server <IPv6>
```

DNS Client IPv6

User can configure an IPv6 dns server IP address.

```
admin@XorPlus# set system dns-server-ip ?
Possible completions:
<IPv4> DNS server IP address <IP>
<IPv6> DNS server IPv6 address <IP>
```

DHCPv6 Client

PicOS supports dhcpv6 function.

Radius over IPv6

User can configure an IPv6 address for the radius server.

```
admin@XorPlus# set system aaa radius authorization server-ip ?
Possible completions:
<IPv4> Radius authorization IPv4 server address
<IPv6> Radius authorization IPv6 server address
```

Configuring NETCONF

NETCONF is a network configuration and management protocol based on XML.

NETCONF protocol uses XML for configuration data and protocol message encoding, using RPC and Client/Server mechanism to update, install or delete the relevant part of the device configuration or all the management information.

- Currently, we support <get>, <get-config>, <get-schema> and <edit-config>.
- Authenticated RADIUS/TACACS+ users can access to PicOS switch via NETCONF.

Enable NETCONF on switch:

```
admin@XorPlus# set protocols netconf
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Delete NETCONF configuration on switch:

```
admin@XorPlus# delete protocols netconf
Deleting:
    netconf {
    }
OK
admin@XorPlus# commit
Commit OK.
Save done.
```

YANG is a data modeling language used to model configuration and state data manipulated by NETCONF.
You can find the YANG module file of different modules on your switch under the directory "/pica/etc/common/data-models".

```
admin@XorPlus$pwd
/pica/etc/common/data-models
admin@XorPlus$ls -lt *.yang
-rw-rw-r-- 1 root xorp  2288 Jul  9 16:14 arp.yang
-rw-rw-r-- 1 root xorp  4075 Jul  9 16:14 bfd.yang
-rw-rw-r-- 1 root xorp  6950 Jul  9 16:14 cos-with-pfc.yang
-rw-rw-r-- 1 root xorp  6062 Jul  9 16:14 cos-without-pfc.yang
-rw-rw-r-- 1 root xorp  3031 Jul  9 16:14 dhcp.yang
-rw-rw-r-- 1 root xorp  5173 Jul  9 16:14 dot1x.yang
-rw-rw-r-- 1 root xorp 14261 Jul  9 16:14 firewall-no-icmp-type-code.yang
-rw-rw-r-- 1 root xorp 14857 Jul  9 16:14 firewall.yang
-rw-rw-r-- 1 root xorp 16760 Jul  9 16:14 ietf-inet-types.yang
-rw-rw-r-- 1 root xorp 18034 Jul  9 16:14 ietf-yang-types.yang
-rw-rw-r-- 1 root xorp  4814 Jul  9 16:14 igmpsnooping.yang
-rw-rw-r-- 1 root xorp  3320 Jul  9 16:14 lacp.yang
-rw-rw-r-- 1 root xorp  6944 Jul  9 16:14 lldp.yang
-rw-rw-r-- 1 root xorp  4492 Jul  9 16:14 mlag.yang
-rw-rw-r-- 1 root xorp 25632 Jul  9 16:14 mstp.yang
-rw-rw-r-- 1 root xorp  4825 Jul  9 16:14 neighbour.yang
-rw-rw-r-- 1 root xorp  1052 Jul  9 16:14 routing.yang
-rw-rw-r-- 1 root xorp  5123 Jul  9 16:14 sflow.yang
-rw-rw-r-- 1 root xorp  4904 Jul  9 16:14 snmp.yang
-rw-rw-r-- 1 root xorp 13185 Nov  4 10:44 static-routes.yang
-rw-rw-r-- 1 root xorp 50887 Jul  9 16:14 system.yang
-rw-rw-r-- 1 root xorp  4126 Jul  9 16:14 udld.yang
-rw-rw-r-- 1 root xorp   871 Jul  9 16:14 version.yang
-rw-rw-r-- 1 root xorp 10137 Nov  4 10:44 vlan-interface.yang
-rw-rw-r-- 1 root xorp  8000 Jul  9 16:14 vlans.yang
-rw-rw-r-- 1 root xorp 11145 Nov  4 10:44 vrrp.yang
-rw-rw-r-- 1 root xorp  8679 Nov  4 10:44 vxlans.yang
```

```
-rw-rw-r-- 1 root xorp  4515 Jul  9 16:14 xovs.yang
```

Example of VLAN configuration via NETCONF use <edit-config>:

Step 1: Create an XML file according the vlan.yang for RPC request to create VLAN136:

```
<vlans xmlns="http://pica8.com/xorplus/vlans">
    <vlan-id>
      <id>136</id>
      <description/>
      <vlan-name>default</vlan-name>
      <l3-interface>vlan136</l3-interface>
    </vlan-id>
  </vlans>
```

Step 2: Display the configuration on switch after the client sending an RPC request.

```
The configuration has been changed by user root
DELTAS:
    vlans {
        vlan-id 136 {
            description: ""
            vlan-name: "default"
            l3-interface: "vlan136"
        }
    }
admin@XorPlus# show | display set
    set protocols netconf
    set vlans vlan-id 136 l3-interface "vlan136"
```

> Now, we only support get the system's version information and vxlan information via NETCONF <get> function.

Example of get the system's version information via NETCONF use <get>:

Display the RPC reply after the client sending an RPC request.

```
   <version xmlns="http://pica8.com/xorpplus/version">
     <mac_address>48:0f:cf:af:70:3b</mac_address>
     <hardware_mode>HP5712</hardware_mode>
     <system_version>2.8.0/aeec598</system_version>
     <system_released_date>10/13/2016</system_released_date>
     <L2_L3_version>2.8.0/aeec598</L2_L3_version>
     <L2_L3_released_date>10/13/2016</L2_L3_released_date>
   </version>
```

NETCONF client

About NETCONF client, you can use ncclient which is python lib now.

> If you use ncclient, you must modify the rpc.py : add two lines codes to work with pica8 switch.
>
> Edit the `rpc.py` file to contain the followings before the statement 'self._session.send(req)':
>
> req = req.replace('nc:','')
>
> req = req.replace(':nc','')

Get .yang or .yin File

The administrator can use get-schema operation to retrieve the **.yang** or **.yin** data file information on the PICA8 switch. For details about get-schema operation, see RFC6022 YANG Module for NETCONF Monitoring.

In the following example, the user builds the **testgetschema.py** script on ncclient. The script uses the get-schema operation to get the information from the **vlans.yang** file on the PICA8 switch.

```
[ncclient] $ vi  testgetschema.py
from ncclient import manager
import sys

host=sys.argv[1]
mgr = manager.connect(host=host, port=830, username='admin', password='pica8', hostkey_verify=False)
```

```
elem = mgr.get_schema(identifier='vlans')
with open("%s.xml" % host, 'w') as f:
    f.write(str(elem))
mgr.close_session()
```

Run the **testgetschema.py** script on ncclient. By issuing the get-schema command and receiving the reply from the PICA8 switch, we can get the **vlans.yang** module file information displayed as follows:

```
module vlans {
    namespace "http://pica8.com/xorplus/vlans";
    prefix vlans;
    // import some basic types
    import ietf-yang-types {
        prefix yang;
    }
    organization "PICA8, Inc";
    description
        "This module is data model for vlans configuration";
    revision 2015-12-25 {
        description "Initial revision.";
    }
    container vlans {
        description
            "Vlan configuration.";
        list vlan-id {
            description
                "VLAN tag identifier, range 1-4094, e.g. 2,3,5-100.";
            key "id";
            leaf id {
                type string;
            }
            leaf description {
                description
                    "Vlan description.";
                type string;
                default "";
            }
            leaf vlan-name {
                description
                    "VLAN name, up to 32 alphanumeric characters in length.";
                type string;
                default "default";
            }
            leaf l3-interface {
                description
                    "Associate a Layer 3 interface with an existing VLAN.";
                type string;
                default "";
            }
            leaf open-flow-enable {
                description
                    "Vlan will be used by open flow, maximum of 200 vlans enabled.";
                type boolean;
                default 'false';
            }
        }
........
  }
}
```

SNMP Configuration

- Configuring SNMPv2
- Configuring SNMPv3
- Configuring SNMP ACL
- Pica8 Private MIB
- Pica8 Public MIB
- SNMP Monitoring and Integration with Zabbix

Configuring SNMPv2

> **NOTE:**
> Once created, the loopback interface will always remain UP. Unlike any VLAN interface which can go down accidentally, the loopback interfaces are more stable and hence a much better choice for the SNMP configuration.
> If the Pica8 switch is used as an SNMP Agent device and communicates with the SNMP NMS through the inband port, it is highly recommended to use the IP address of the route reachable loopback interface on the Pica8 switch as the communication address for Snmpwalk, which will ensure that communication is not interrupted and provide stablibility to the SNMP process.

Configuring SNMPv2 Parameters

By default, SNMP is disabled. You can enable SNMP and configure its parameters (e.g. community, contact, location).

You can configure the source interface on the device from which traps are sent. The system specifies the IP address of this interface as the source IP address of traps. In this way, the trap source can be identified on the NMS. To ensure device security, it is recommended that you set the source interface to the loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.10.1.201 prefix-length 32
admin@XorPlus# set protocols snmp community Pica8-data-center
admin@XorPlus# set protocols snmp community Pica8-data-center authorization read-only
admin@XorPlus# set protocols snmp contact support@pica8.com
admin@XorPlus# set protocols snmp location Beijing
admin@XorPlus# set protocols snmp trap-group targets 10.10.1.1 security-name Pica8-data-center
admin@XorPlus# set protocols snmp trap-group version v2
admin@Xorplus# set protocols snmp trap-group source-interface loopback
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

> **In version 2.8.1,security-name has to be configured for trap-group targets whichever the version is .**

Configuring an SNMP ACL

By default, all hosts can *snmpwalk* the information of the switch. Configure an SNMP ACL to control which hosts within the subnetwork can snmpwalk the switch.

```
admin@XorPlus# set system snmp-acl network 1.1.1.0/24
admin@XorPlus# set system snmp-acl network 2.2.2.0/24
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring SNMPset

User can use "snmpset" (OID1.3.6.1.4.1.35098.2.0.0) to load a configuration and can use "snmpset" (OID 1.3.6.1.4.1.35098.2.1.0) to delete or load a configuration. However, only set and delete commands can be included in the command batch (which is OID 1.3.6.1.4.1.35098.2.1.0). Other commands are invalid and ignored. Note that clearing a dependent configuration is not allowed.

```
admin@XorPlus# set protocols snmp community private authorization read-write
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Using snmpset to load a filter configuration:

```
root@dev:~# snmpset -v 2c -c private IP .1.3.6.1.4.1.35098.2.0.0 s "tftp:1.1.5.1:/pica8/acl.conf"
iso.3.6.1.4.1.35098.2.0.0 = STRING: "tftp:1.1.5.1:/pica8/acl.conf"
```

Using snmpset to delete a filter configuration:

```
root@dev:~# snmpset -v 2c -c private IP .1.3.6.1.4.1.35098.2.1.0 s "tftp:1.1.5.1:/pica8/delete-acl.conf"
iso.3.6.1.4.1.35098.2.0.0 = STRING: "tftp:1.1.5.1:/pica8/delete-acl.conf"
```

Enable or Disable LLDP SNMP Trap

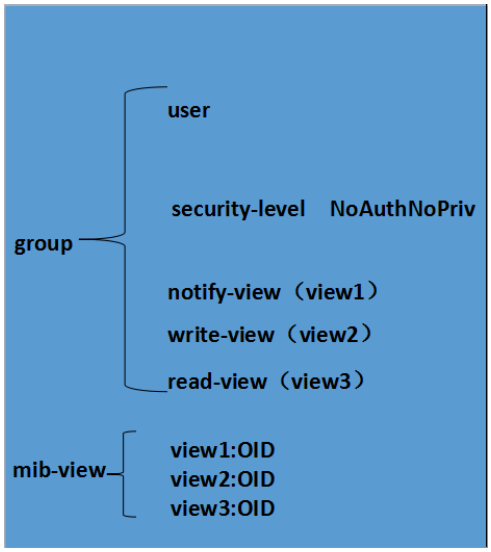
The LLDP SNMP trap is enabled by default. You can use the following command to disable LLDP SNMP trap, then there will be no more LLDP trap message sends to snmp.

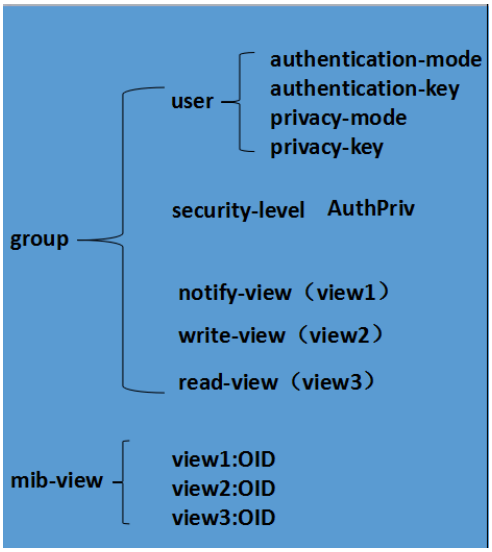
```
admin@Xorplus# set protocols lldp snmp-trap false
admin@Xorplus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

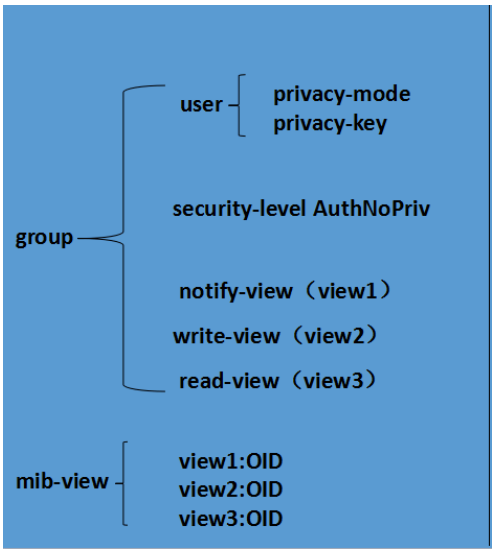
Configuring SNMPv3

Here is the configuration relation diagram in SNMPv3.A user can be added to a group or not as you need.Once a user joined a group,one or more kinds of views (notfiy-view, write-view, read-view) must be configured.Besides, configurations on user change with the security-level of the group as below 3 diagrams. Note notify-view,write-view and read-view are optional but you have to choose at least one view.In the below diagram,view1,view2,view3 can be the same or different.

> **NOTE:**
> Once created, the loopback interface will always remain UP. Unlike any VLAN interface which can go down accidentally, the loopback interfaces are more stable and hence a much better choice for the SNMP configuration.
> If the Pica8 switch is used as an SNMP Agent device and communicates with the SNMP NMS through the inband port, it is highly recommended to use the IP address of the route reachable loopback interface on the Pica8 switch as the communication address for Snmpwalk, which will ensure that communication is not interrupted and provide stablibility to the SNMP process.







Configuring Basic Information

Contact and location information can be configured as below which is the same as SNMPv2.

```
admin@XorPlus# set protocols snmp contact support@pica8.com
admin@XorPlus# set protocols snmp location beijing
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring trap-group

By default, trap messages are sent in the form of SNMPv2. But you can change it to SNMPv3 as below and designate NMS to which trap messages are sent. Note that in SNMPv3, security-name is user while in SNMPv2, security-name is community.

You can configure the source interface on the device from which traps are sent. The system specifies the IP address of this interface as the source IP address of traps. In this way, the trap source can be identified on the NMS. To ensure device security, it is recommended that you set the source interface to the loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.226.14.201 prefix-length 32
admin@XorPlus# set protocols snmp trap-group version v3
admin@XorPlus# set protocols snmp trap-group targets 10.10.51.42 security-name user1
admin@Xorplus# set protocols snmp trap-group source-interface loopback
admin@XorPlus# commit
Commit OK.
Save done.
```

Setting Up a User

By default, SNMPv3 is enabled. And you should set up a usm-user first before you configure other functions of SNMPv3. Besides, adding a user to a group is optional. When a user is added to a group, the needed views should be configured. If you create a user without adding to any groups, you can configure as below. However, under the below circumstance, all the OIDs can be visited by its NMS which can read but can't write and be notified.

```
admin@XorPlus# set protocols snmp v3 usm-user user1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Mib-view

If you want to improve security, the user needs to be added to a group. Because in this way, you can configure a read-view, write-view or notify-view(you can choose only one kind or more as you need) which defines the authority of a NMS. Before configuring a read-view(write-view or notify-view), please set up a mib-view which is used as a view of the group. Here are the configurations. As for a mib-view, you can include or exclude some subtrees and can also configure mask for them.

```
admin@XorPlus# set protocols snmp v3 usm-user user2 group group1
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 type included
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1.6.13 type excluded
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 mask fc
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1.6.13 mask ff
admin@XorPlus# set protocols snmp v3 group group1 read-view view1
admin@XorPlus# set protocols snmp v3 group group1 write-view view1
admin@XorPlus# set protocols snmp v3 group group1 notify-view view1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Security-level

You can improve security better by configuring security-level for the group. And the default setting of security-level is NoAuthNoPriv. You can change it to AuthNoPriv or AuthPriv. But please remember to configure authentication-mode, authentication-key, privacy-mode, privacy-key for the user. Configuration are as below.

```
admin@XorPlus# set protocols snmp v3 group group1 security-level AuthPriv
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-mode md5
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-key authnkey
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-mode des
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-key privykey
admin@XorPlus# commit
Commit OK.
Save done.
```

NMS Visits Switch by user

NMS reads OID tree 1.3.6.1.2.1.6.13 as below. user1 is the user's name. AuthPriv is the security-level of group. 10.10.51.155 is the IP of the switch.

```
pica8@pica8:~$snmpwalk -u user1 -l AuthPriv -A sha -a u1111key -X des -x u1111key 10.10.51.155 1.3.6.1.2.1.6.13
```

Enable or Disable LLDP SNMP Trap

The LLDP SNMP trap is enabled by default. You can use the following command to disable LLDP SNMP trap, then there will be no more LLDP trap message sends to snmp.

```
admin@Xorplus# set protocols lldp snmp-trap false
admin@Xorplus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Configuring SNMP ACL

- Concepts
- Matching Procedure
- Examples
  - Example 1
  - Example 2
  - Example 3

By default, no SNMP ACL list is configured on the switch and allows all network management station (NMS) to access the device through SNMP protocol. Users can configure access control white list for SNMP protocol on the device to restrict NMS access to the device, so as to improve the device security.

Concepts

SNMP ACL has two types of access control white list: As-per User List and Global List.

- As-per User List

The SNMP ACL that specifies the security name can be configured with multiple networks, is called the as-per user list. For example,

```
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.50.0/24
```

Where "security-name" is the **community name** for SNMPv1 and SNMPv2, and the **usm-user** name in command **set protocols snmp v3 usm-user** *<user-name>* for SNMPv3.

- Global List

SNMP ACLs that do not specify a security name but only networks are called the global list. For example,

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl network 10.10.51.0/24
```

The global list is applied to NMS that are not configured with an as-per user list.

Matching Procedure

As-per user list and global list can be configured together. The matching procedure for SNMP ACL is as follows:

1. For the NMS that accesses the device (assuming its security name is ***s1***), if a valid as-per user list is configured on the device (i.e., an SNMP ACL with security name ***s1*** and network is configured), as-per user list matching is performed.

- If the SNMP query matches the as-per user list, allowing NMS to access to devices through SNMP protocol.
- If no as-per user list entry is matched, the NMS who sent the SNMP query is denied access to this device.

NOTE:

If an SNMP ACL with security name s1 is configured, but no network list is configured under it, the as-per user list is empty and invalid, then global list matching will be performed.

2. If no as-per user list is configured for this NMS (i.e., the SNMP ACL with security name ***s1*** is not configured), then global list matching is performed.

- If the SNMP query matches a global list, allowing NMS to access devices through SNMP protocol.
- If no global list entry is matched, the NMS who sent the message is denied access to this device.
- If global list is not configured then the NMS is allowed to access the device through SNMP protocol.

Examples

Three examples are given to illustrate the SNMP ACL procedure.

Example 1

The following configurations were set on the switch:

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.51.0/24
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.52.0/24
```

- In case of ***user1***, SNMP queries from 10.10.10.51.0/24 and 10.10.52.0/24 are allowed to go to SNMP agent. And others will be denied.
- For other users, only SNMP queries from 10.10.50.0/24 (SNMP ACL global list configuration) are accepted.

Example 2

The following configurations were set on the switch:

```
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.11.0/24
```

```
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.12.0/24
```

- In case of ***user1***, SNMP queries from 10.10.10.11.0/24 and 10.10.12.0/24 are allowed to go to SNMP agent. And others will be denied.
- For other users, SNMP queries will be accepted by SNMP agent, as SNMP ACL global list configuration is NULL.

Example 3

The following configurations were set on the switch:

```
! SNMPv3 user pica8test123
    admin@XorPlus# set protocols snmp v3 mib-view readall subtree 1 mask ff
    admin@XorPlus# set protocols snmp v3 group Pica8 security-level AuthPriv
    admin@XorPlus# set protocols snmp v3 group Pica8 read-view readall
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 group Pica8
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 authentication-mode md5
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 authentication-key P3Ca8536bl4
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 privacy-mode des
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 privacy-key P3Ca8536bl8
    admin@XorPlus# set system snmp-acl security-name pica8test123 network 192.168.42.0/24


! SNMPv3 user pica8test321
    admin@XorPlus# set protocols snmp v3 mib-view readall subtree 1 mask ff
    admin@XorPlus# set protocols snmp v3 group Pica8 security-level AuthPriv
    admin@XorPlus# set protocols snmp v3 group Pica8 read-view readall
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 group Pica8
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 authentication-mode md5
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 authentication-key P3Ca8536bl4
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 privacy-mode des
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 privacy-key P3Ca8536bl8
    admin@XorPlus# set system snmp-acl security-name pica8test321 network 192.168.43.0/24
```

- Get switch model using SNMPv3 from an NMS IP located in the 172.168.42.0/24 network using the *pica8test123* user credentials. The expected result is: Switch model for switch at IP *192.168.42.171* is provided.

```
admin@NMS# snmpwalk -v3 -u pica8test123 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171 1.3
iso.3.6.1.4.1.35098.1.13.0 = STRING: "N3248P-ON"
```

- Get switch model using SNMP v3 from an NMS IP located in the 172.168.42.0/24 network using the *pica8test321* user credentials. Switch model for switch at IP *192.168.42.171* is not provided. The requesting SNMP server IP is not in 192.168.43.0/24 network, hence it is not allowed to get the switch model.

```
admin@NMS# snmpwalk -v3 -u pica8test321 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171 1.3
Timeout: No Response from 192.168.42.171
```

- After deleting SNMP ACL for pica8test321, it is able to get the hardware model:

```
admin@NMS# snmpwalk -v3 -u pica8test321 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171 1.3
iso.3.6.1.4.1.35098.1.13.0 = STRING: "N3248P-ON"
```

Pica8 Private MIB

Pica8 added some private and trap MIBs listed below:

1：**SNMP Trap list:**

(1) **lldpStatistics**：1.0.8802.1.1.2.1.2

(2) **Ospf**：1.3.6.1.2.1.14

(3) **link up**: OID: 1.3.6.1.6.3.1.1.5.4

link down:OID:1.3.6.1.6.3.1.1.5.3

(support physical port's link up/down and lag port up/down)

(4) **Rpsu trap** :1.3.6.1.4.1.35098.21.1

(rpsu plugged in/out , rpsustatechange-power on/off, rpsuFanFailed)
oidRpsuFanFailed 1.3.6.1.4.1.35098.21.1.4
oidRpsuFanRecovery 1.3.6.1.4.1.35098.21.1.7
oidRpsuStateChange 1.3.6.1.4.1.35098.21.1.1
oidRpsuPlugIn 1.3.6.1.4.1.35098.21.1.2
oidRpsuPlugOut 1.3.6.1.4.1.35098.21.1.3
oidRpsuFanFailed 1.3.6.1.4.1.35098.21.1.4
oidRpsuStatusChangePowerOff 1.3.6.1.4.1.35098.21.1.5
oidRpsuStatusChangePowerOn 1.3.6.1.4.1.35098.21.1.6
oidRpsuFanRecovery 1.3.6.1.4.1.35098.21.1.7

(5) **Sfp trap**: 1.3.6.1.4.1.35098.21.2 (plugged in /out)

(6) **Warm start** : OID:1.3.6.1.6.3.1.1.5.2

Cold start: OID:1.3.6.1.6.3.1.1.5.1

oidCpuHighThreshold 1.3.6.1.4.1.35098.21.4.1

oidCpuLowThreshold 1.3.6.1.4.1.35098.21.4.2

oidMacThreshold 1.3.6.1.4.1.35098.21.5.1

(7) **FAN trap**
oidSwitchFanFailed 1.3.6.1.4.1.35098.21.3.1
oidSwitchFanPlugIn 1.3.6.1.4.1.35098.21.3.2
oidSwitchFanPlugOut 1.3.6.1.4.1.35098.21.3.3
oidSwitchFanRecovery 1.3.6.1.4.1.35098.21.3.4

2：**pica8 private mib:**

cpuUsage OID 1.3.6.1.4.1.35098.1.1

totalPhyMemory 1.3.6.1.4.1.35098.1.2

usedPhyMemory 1.3.6.1.4.1.35098.1.3

freePhyMemory 1.3.6.1.4.1.35098.1.4

switchTemperature 1.3.6.1.4.1.35098.1.5

cpuTemperature 1.3.6.1.4.1.35098.1.6

switchChipTemperature 1.3.6.1.4.1.35098.1.7

switchFanSpeed 1.3.6.1.4.1.35098.1.8

switchPWM 1.3.6.1.4.1.35098.1.9

sfpstatusEntry 1.3.6.1.4.1.35098.1.10.1

sfpIndex 1.3.6.1.4.1.35098.1.10.1.1

sfpVendorName 1.3.6.1.4.1.35098.1.10.1.2

sfpSerialNumber 1.3.6.1.4.1.35098.1.10.1.3

sfpTemp 1.3.6.1.4.1.35098.1.10.1.4

sfpVoltage 1.3.6.1.4.1.35098.1.10.1.5

sfpBias 1.3.6.1.4.1.35098.1.10.1.6

sfpTxPower 1.3.6.1.4.1.35098.1.10.1.7

sfpRxPower 1.3.6.1.4.1.35098.1.10.1.8

sfpType 1.3.6.1.4.1.35098.1.10.1.9

rpsustatusEntry 1.3.6.1.4.1.35098.1.11.1

rpsuIndex 1.3.6.1.4.1.35098.1.11.1.1

serialNumber 1.3.6.1.4.1.35098.1.11.1.2

rpsuStatus 1.3.6.1.4.1.35098.1.11.1.3

rpsuTemprature 1.3.6.1.4.1.35098.1.11.1.4

rpsuFanSpeed 1.3.6.1.4.1.35098.1.11.1.5

rpsuPWM 1.3.6.1.4.1.35098.1.11.1.6

fanstatusEntry 1.3.6.1.4.1.35098.1.12.1

fanIndex 1.3.6.1.4.1.35098.1.12.1.1

fanStatus 1.3.6.1.4.1.35098.1.12.1.2

fanFail 1.3.6.1.4.1.35098.1.12.1.3

fanSpeed 1.3.6.1.4.1.35098.1.12.1.4

fanPWM 1.3.6.1.4.1.35098.1.12.1.5

oidCpuThresholdStatus 1.3.6.1.4.1.35098.1.14.1.0

oidCpuHighThresholdValue 1.3.6.1.4.1.35098.1.14.2.0

oidCpuLowThresholdValue 1.3.6.1.4.1.35098.1.14.3.0

oidCpuThresholdPeriod 1.3.6.1.4.1.35098.1.14.4.0

oidMacThresholdStatus 1.3.6.1.4.1.35098.1.15.1.0

oidMacThresholdValue 1.3.6.1.4.1.35098.1.15.2.0

oidMacThresholdPeriod 1.3.6.1.4.1.35098.1.15.3.0

oidMacMonitorValue 1.3.6.1.4.1.35098.1.15.4.0

- pica_private_mib.my
- pica_private_trap_mib.my

pica_private_mib.my

File Download:

pica_private_mib.my

The following is the details of the *pica_private_mib.my* file.

```
PICA-PRIVATE-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32, Counter64,
Integer32, Unsigned32, TimeTicks, mib-2, snmpModules,IpAddress,
NOTIFICATION-TYPE FROM SNMPv2-SMI
TEXTUAL-CONVENTION, DisplayString,
PhysAddress, TruthValue, RowStatus,
TimeStamp, AutonomousType, TestAndIncr FROM SNMPv2-TC
MODULE-COMPLIANCE, OBJECT-GROUP,
NOTIFICATION-GROUP FROM SNMPv2-CONF
snmpTraps FROM SNMPv2-MIB
IANAifType FROM IANAifType-MIB
enterprises FROM RFC1155-SMI;

picaPrivateMib MODULE-IDENTITY
LAST-UPDATED "201104280000Z"
ORGANIZATION "Pica8 Inc."
CONTACT-INFO
" Customer Support
E-Mail: support@pica8.com
WWW: http://www.pica8.com"
DESCRIPTION
"The MIB module to manage Pica8's Pronto product."
REVISION
"201104280000Z"
DESCRIPTION
"The Pica8 Private MIB, Initial Version.
Author: Robin Wan."

::= { enterprises 35098 }

hostStatusGroup OBJECT IDENTIFIER ::= { picaPrivateMib 1 }

cpuUsage OBJECT-TYPE
SYNTAX INTEGER(0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The usage of CPU, the output format is integer."
::= { hostStatusGroup 1 }

totalPhyMemory OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The total physical memory size, the output format is string."
::= { hostStatusGroup 2 }

usedPhyMemory OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The used physical memory size, the output format is string."
::= { hostStatusGroup 3 }

freePhyMemory OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The free physical memory size, the output format is string."
::= { hostStatusGroup 4 }

switchTemperature OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The temperature of switch, the output format is integer."
::= { hostStatusGroup 5 }

cpuTemperature OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The temperature of CPU, the output format is integer."
::= { hostStatusGroup 6 }

switchChipTemperature OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The temperature of switch chip."
::= { hostStatusGroup 7 }

switchFanSpeed OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The fan speed of switch chip."
::= { hostStatusGroup 8 }

switchPWM OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Pulse Width Modulation(PWM) of switch chip."
::= { hostStatusGroup 9 }

sfpstatusTable OBJECT-TYPE
SYNTAX SEQUENCE OF SfpstatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A list of SFP moudule status entries."
::= { hostStatusGroup 10 }

sfpstatusEntry OBJECT-TYPE
SYNTAX SfpstatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry containing all SFP module status"
INDEX { sfpIndex }
::= { sfpstatusTable 1 }

SfpstatusEntry ::=
SEQUENCE {
sfpIndex INTEGER,
sfpVendorName DisplayString,
sfpSerialNumber DisplayString,
sfpTemp DisplayString,
```

```
sfpVoltage DisplayString,
sfpBias DisplayString,
sfpTxPower DisplayString,
sfpRxPower DisplayString,
sfpType DisplayString,
sfpPartNumber DisplayString
}

sfpIndex OBJECT-TYPE
SYNTAX INTEGER (1..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The port number of interface."
::= { sfpstatusEntry 1 }

sfpVendorName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The vendor name of SFP transceiver."
::= { sfpstatusEntry 2 }

sfpSerialNumber OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The serial number of SFP transceiver."
::= { sfpstatusEntry 3 }

sfpTemp OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The temperature of SFP transceiver."
::= { sfpstatusEntry 4 }

sfpVoltage OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The voltage of SFP transceiver."
::= { sfpstatusEntry 5 }

sfpBias OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The bias current of SFP transceiver."
::= { sfpstatusEntry 6 }

sfpTxPower OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The TX power of SFP transceiver (dBm)."
::= { sfpstatusEntry 7 }

sfpRxPower OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The RX power of SFP transceiver (dBm)."
```

```
::= { sfpstatusEntry 8 }

sfpType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The type of SFP transceiver."
::= { sfpstatusEntry 9 }

sfpPartNumber OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The part number of SFP transceiver."
::= { sfpstatusEntry 10 }

rpsustatusTable OBJECT-TYPE
SYNTAX SEQUENCE OF RpsustatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A list of redundant power supply unit(RPSU) status entries."
::= { hostStatusGroup 11 }
rpsustatusEntry OBJECT-TYPE
SYNTAX RpsustatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry containing redundant power supply unit(RPSU) status."
INDEX { rpsuIndex }
::= { rpsustatusTable 1 }

RpsustatusEntry ::=
SEQUENCE {
rpsuIndex INTEGER,
serialNumber DisplayString,
rpsuStatus INTEGER,
rpsuTemperature DisplayString,
rpsuFanSpeed INTEGER
}
rpsuIndex OBJECT-TYPE
SYNTAX INTEGER(0..10)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The slot number of redundant power supply unit (RPSU)."
::= { rpsustatusEntry 1 }

serialNumber OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The serial number of redundant power supply unit (RPSU)."
::= { rpsustatusEntry 2 }

rpsuStatus OBJECT-TYPE
SYNTAX INTEGER (0..1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The status of redundant power supply unit(RPSU).
1: The redundant power supply unit(RPSU) power on.
0: The redundant power supply unit(RPSU) power off."
::= { rpsustatusEntry 3 }

rpsuTemperature OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Temprature of the redundant power supply unit (RPSU)."
::= { rpsustatusEntry 4 }

rpsuFanSpeed OBJECT-TYPE
SYNTAX INTEGER(1..2147483647)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Fan speed of the redundant power supply unit (RPSU)."
::= { rpsustatusEntry 5 }

fanStatusTable OBJECT-TYPE
SYNTAX SEQUENCE OF FanStatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A list of Fan status entries."
::= { hostStatusGroup 12 }
fanstatusEntry OBJECT-TYPE
SYNTAX FanStatusEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry containing fan status."
INDEX { fanIndex }
::= { fanStatusTable 1 }

FanStatusEntry ::=
SEQUENCE {
fanIndex INTEGER,
fanStatus INTEGER,
fanFail INTEGER,
fanSpeed DisplayString,
fanPWM DisplayString
}
fanIndex OBJECT-TYPE
SYNTAX INTEGER(0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The fan number."
::= { fanstatusEntry 1 }

fanStatus OBJECT-TYPE
SYNTAX INTEGER (0..1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The status of Fan.
1: The fan is present.
0: The fan is not present."
::= { fanstatusEntry 2 }

fanFail OBJECT-TYPE
SYNTAX INTEGER (0..1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Fan of switch chip fails or not.
1: Fan fail.
0: Fan not fail."
::= { fanstatusEntry 3 }

fanSpeed OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
```

```
DESCRIPTION
"The fan speed of switch chip."
::= { fanstatusEntry 4 }

fanPWM OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Pulse Width Modulation(PWM) of switch chip fan."
::= { fanstatusEntry 5 }

platformName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The platform name of the switch."
::= { hostStatusGroup 13 }


cpuThreshold OBJECT IDENTIFIER ::= { hostStatusGroup 14 }

cpuThresholdStatus OBJECT-TYPE
SYNTAX INTEGER (0..1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The enable status for CPU threshold.
1: The CPU threshold is enabled.
0: The CPU threshold is disabled."
DEFVAL { 0 }
::= { cpuThreshold 1 }

cpuHighThresholdValue OBJECT-TYPE
SYNTAX Unsigned32 (1..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The percentage high threshold value configured by
the user. The value indicates,
if the total CPU utilization is equal to or above
this value for cpuThresholdPeriod duration,
then send a cpuHighThreshold notification to the NMS."
DEFVAL { 80 }
::= { cpuThreshold 2 }

cpuLowThresholdValue OBJECT-TYPE
SYNTAX Unsigned32 (1..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The percentage low threshold value configured by the user.
The value indicates, if the total CPU utilization is equal to
or below this value for cpuThresholdPeriod duration,
then send a cpuLowThreshold notification to the NMS."
DEFVAL { 20 }
::= { cpuThreshold 3 }

cpuThresholdPeriod OBJECT-TYPE
SYNTAX Unsigned32 (5..4294967295)
UNITS "seconds"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This is an observation interval. This value indicates,
if the total CPU utilization is above or equal to the
cpuHighThresholdValue for this duration, or if the
the total CPU utilization is be equal to or below the
cpuLowThresholdValue for this duration, then send a
```

```
cpuHighThreshold/cpuLowThreshold notification
to the NMS."
DEFVAL { 300 }
::= { cpuThreshold 4 }



macThreshold OBJECT IDENTIFIER ::= { hostStatusGroup 15 }

macThresholdStatus OBJECT-TYPE
SYNTAX INTEGER (0..1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The enable status for mac address table threshold.
1: The mac address table threshold is enabled.
0: The mac address table threshold is disabled."
DEFVAL { 0 }
::= { macThreshold 1 }

macThresholdValue OBJECT-TYPE
SYNTAX Unsigned32 (1..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The percentage of maximum mac address table capacity
configured by the user. The value indicates,
if the mac address table usage is equal to or
above this value for macThresholdPeriod duration,
then send a macThreshold notification to the NMS."
DEFVAL { 50 }
::= { macThreshold 2 }

macThresholdPeriod OBJECT-TYPE
SYNTAX Unsigned32 (5..4294967295)
UNITS "minutes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This is an observation interval.The value indicates,
if the mac address table usage percentage is equal to
or above the macThresholdValue for this duration, then
send a macThreshold notification to the NMS."
DEFVAL { 15 }
::= { macThreshold 3 }

macMonitorValue OBJECT-TYPE
SYNTAX Unsigned32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The overall mac address table usage percentage in the
last macThreshold notification to the NMS."
::= { macThreshold 4 }

motherBoardSerialNumber OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The serial number of the motherboard."
::= { hostStatusGroup 16 }

hardwareId OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The hardware id information."
::= { hostStatusGroup 17 }
```

```
switchConfigGroup OBJECT IDENTIFIER ::= { picaPrivateMib 2 }

tftpConfigFilePath OBJECT-TYPE
SYNTAX OCTET STRING (SIZE (2..255))
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"If the tftp path of defined config file is set, the configurations
included in the config file are also applied meanwhile. "
::= { switchConfigGroup 0 }

tftpBatchFilePath OBJECT-TYPE
SYNTAX OCTET STRING (SIZE (2..255))
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"If the tftp path of a command batch file is set, the present configurations
will be changed depending on the execution of the commands in the batch file."
::= { switchConfigGroup 1 }

picaConformance OBJECT IDENTIFIER ::= { picaPrivateMib 20}
picaGroups OBJECT IDENTIFIER ::= { picaConformance 1 }
picaCompliances OBJECT IDENTIFIER ::= { picaConformance 2 }

picaBasicGroup OBJECT-GROUP
OBJECTS {
cpuUsage,
totalPhyMemory,
usedPhyMemory,
freePhyMemory,
switchTemperature,
cpuTemperature,
switchChipTemperature,
switchFanSpeed,
switchPWM,
platformName,
motherBoardSerialNumber,
hardwareId
}
STATUS current
DESCRIPTION
"These objects are required for pica private mib."
::= { picaGroups 1 }
picasfpGroup OBJECT-GROUP
OBJECTS {
sfpIndex,
sfpVendorName,
sfpSerialNumber,
sfpTemp,
sfpVoltage,
sfpBias,
sfpTxPower,
sfpRxPower,
sfpType,
sfpPartNumber
}
STATUS current
DESCRIPTION
"These objects are required for pica private mib."
::= { picaGroups 2 }

picarpsuGroup OBJECT-GROUP
OBJECTS {
rpsuIndex,
serialNumber,
rpsuStatus,
rpsuTemperature,
rpsuFanSpeed
}
```

```
STATUS current
DESCRIPTION
" These objects are required for pica private mib."
::= { picaGroups 3 }

picaConfigGroup OBJECT-GROUP
OBJECTS {
tftpConfigFilePath,
tftpBatchFilePath
}
STATUS current
DESCRIPTION
" These objects are required for pica private mib."
::= {picaGroups 4 }

picaFanGroup OBJECT-GROUP
OBJECTS {
fanIndex,
fanStatus,
fanFail,
fanSpeed,
fanPWM
}
STATUS current
DESCRIPTION
" These objects are required for pica private mib."
::= {picaGroups 5 }

cpuThresholdGroup OBJECT-GROUP
OBJECTS {
cpuThresholdStatus,
cpuHighThresholdValue,
cpuLowThresholdValue,
cpuThresholdPeriod
}
STATUS current
DESCRIPTION
" These objects are required for pica private mib."
::= {picaGroups 6 }

macThresholdGroup OBJECT-GROUP
OBJECTS {
macThresholdStatus,
macThresholdValue,
macThresholdPeriod,
macMonitorValue
}
STATUS current
DESCRIPTION
" These objects are required for pica private mib."
::= {picaGroups 7 }

picaCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement "
MODULE -- this module
MANDATORY-GROUPS {
picaBasicGroup,
picasfpGroup,
picarpsuGroup,
picaConfigGroup,
picaFanGroup,
cpuThresholdGroup
}
::= { picaCompliances 1 }

END
```

pica_private_trap_mib.my

File Download:

pica_private_trap_mib.my

The following is the details of the *pica_private_trap_mib.my* file.

```
PICA-PRIVATE-TRAP-MIB DEFINITIONS ::= BEGIN

    IMPORTS
            MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, IpAddress
                FROM SNMPv2-SMI
            MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
                FROM SNMPv2-CONF
            rpsuIndex, rpsuStatus,sfpIndex,fanIndex,picaPrivateMib,
            cpuHighThresholdValue, cpuLowThresholdValue,
            cpuUsage, macThresholdValue, macMonitorValue
                FROM PICA-PRIVATE-MIB;

    picaTrap MODULE-IDENTITY
           LAST-UPDATED "201212290000Z"
           ORGANIZATION "Pica8 Inc."
           CONTACT-INFO
            "                       Customer Support
            E-Mail:                 support@pica8.com
            WWW:                    http://www.pica8.com"
       DESCRIPTION
          "The MIB module to describe traps for pica private mib."
      ::= { picaPrivateMib 21 }

-- Trap Support Objects

--         The following are support objects for the pica private traps.


rpsuTraps OBJECT IDENTIFIER ::= { picaTrap 1 }
spfTraps OBJECT IDENTIFIER ::= { picaTrap 2 }
switchTraps OBJECT IDENTIFIER ::= { picaTrap 3 }
cpuThresholdTraps OBJECT IDENTIFIER ::= { picaTrap 4 }
macThresholdTraps OBJECT IDENTIFIER ::= { picaTrap 5 }

-- Traps

   switchFanFailed NOTIFICATION-TYPE
        OBJECTS {
                    fanIndex -- The number of fan
                  }
        STATUS             current
        DESCRIPTION
           "A switchFanFailed trap will be generated if a switch fan
           fails."
   ::= { switchTraps 1 }

   switchFanPlugIn NOTIFICATION-TYPE
        OBJECTS {
                    fanIndex -- The number of fan
                  }
        STATUS             current
        DESCRIPTION
           "A switchFanPlugIn trap signifies that
           the fan is plugged in."
   ::= { switchTraps 2 }

   switchFanPlugOut NOTIFICATION-TYPE
        OBJECTS {
                    fanIndex -- The number of fan
```

```
                }
     STATUS             current
     DESCRIPTION
        "A switchFanPlugOut trap signifies that
        the fan is plugged out."
::= { switchTraps 3 }

switchFanRecovery NOTIFICATION-TYPE
     OBJECTS {
                fanIndex -- The number of fan
                }
     STATUS             current
     DESCRIPTION
        "A switchFanRecovery trap will be generated if the fan
        of switch recovers from failure."
::= { switchTraps 4 }

rpsuStateChange NOTIFICATION-TYPE
     OBJECTS {
                rpsuIndex, -- The number of RPSU
                rpsuStatus   -- The new state
                }
     STATUS             current
     DESCRIPTION
        "An rpsuStateChange trap signifies that there
        has been a change in the state of a redundant
        power supply unit (RPSU). This trap should  be
        generated when the RPSU status changes (e.g.,
        plugged in or out)."
::= { rpsuTraps 1 }

rpsuPlugIn NOTIFICATION-TYPE
     OBJECTS {
                rpsuIndex -- The number of RPSU
                }
     STATUS             current
     DESCRIPTION
         "An rpsuPlugIn trap will be generated if a
          redundant power supply unit (RPSU) is plugged in."
::= { rpsuTraps 2 }

rpsuPlugOut NOTIFICATION-TYPE
     OBJECTS {
                rpsuIndex  -- The number of RPSU
                }
     STATUS             current
     DESCRIPTION
        "An rpsuPlugOut trap will be generated if a
        redundant power supply unit (RPSU) is plugged out."
::= { rpsuTraps 3 }

rpsuFanFailed NOTIFICATION-TYPE
     OBJECTS {
                rpsuIndex  -- The number of RPSU
                }
     STATUS             current
     DESCRIPTION
        "An rpsuFanFailed trap will be generated if a fan
        of Redundant power supply unit (RPSU) has failed."
::= { rpsuTraps 4 }

rpsuStatusChangePowerOff NOTIFICATION-TYPE
     OBJECTS {
                rpsuIndex -- The number of RPSU
                }
     STATUS             current
     DESCRIPTION
        "An rpsuStatusChangePowerOff trap signifies that
        the RPSU status changed to power off."
::= { rpsuTraps 5 }
```

```
 rpsuStatusChangePowerOn NOTIFICATION-TYPE
      OBJECTS {
                  rpsuIndex -- The number of RPSU
                }
      STATUS              current
      DESCRIPTION
         "An rpsuStatusChangePowerOn trap signifies that
         the RPSU status changed to power on."
 ::= { rpsuTraps 6 }

rpsuFanRecovery NOTIFICATION-TYPE
      OBJECTS {
                  rpsuIndex  -- The number of RPSU
                }
      STATUS              current
      DESCRIPTION
         "An rpsuFanRecovery trap will be generated if the fan
         of the redundant power supply unit (RPSU) recovers from failure."
 ::= { rpsuTraps 7 }

 sfpPlugIn NOTIFICATION-TYPE
      OBJECTS {
                  sfpIndex -- The index of SFP
                }
      STATUS              current
      DESCRIPTION
          "An sfpPlugIn trap signifies the SFP is plugged in."
 ::= { spfTraps 1 }

 sfpPlugOut NOTIFICATION-TYPE
      OBJECTS {
                  sfpIndex  -- The index of SFP
                }
      STATUS              current
      DESCRIPTION
         "A sfpPlugOut trap signifies the SFP is plugged out."
 ::= { spfTraps 2 }

 cpuHighThreshold NOTIFICATION-TYPE
      OBJECTS {
                  cpuHighThresholdValue,
                  cpuUsage
                }
      STATUS              current
      DESCRIPTION
         "A cpuHighThreshold notification is sent
         when configured high CPU utilization threshold
         (cpuHighThresholdValue) is reached and
         CPU utilization remained above the threshold
         for configured interval(cpuThresholdPeriod)
         and such a notification is requested."
 ::= { cpuThresholdTraps 1 }

 cpuLowThreshold NOTIFICATION-TYPE
      OBJECTS {
                  cpuLowThresholdValue,
                  cpuUsage
                }
      STATUS           current
      DESCRIPTION
         "A cpuLowThreshold is sent when the configured
         low threshold (cpuLowThresholdValue) is
         reached and CPU utilization remained under threshold
         for configured interval (cpuThresholdPeriod)
         and such a notification is requested."
 ::= { cpuThresholdTraps 2 }

 macThreshold NOTIFICATION-TYPE
      OBJECTS {
```

```
                    macThresholdValue,
                    macMonitorValue
                  }
        STATUS          current
        DESCRIPTION
           "A macThreshold is sent when the configured mac
           address table threshold (macThresholdValue) is
           reached and mac address usage percentage remained
           above the threshold for configured interval
           (macThresholdPeriod) and such a notification
           is requested."
   ::= { macThresholdTraps 1 }


picaTrapConformance OBJECT IDENTIFIER ::= { picaTrap 20 }

picaTrapGroups      OBJECT IDENTIFIER ::= { picaTrapConformance 1 }
picaTrapCompliances OBJECT IDENTIFIER ::= { picaTrapConformance 2 }

-- compliance statements

    picaTrapCompliance MODULE-COMPLIANCE
        STATUS  current
        DESCRIPTION
           "The compliance statement "
       MODULE  -- this module
        GROUP       picaTrapGroups
        DESCRIPTION
           "This group is optional but recommended"
       ::= { picaTrapCompliances 1 }


-- units of conformance

    rpusTrapGroup    OBJECT-GROUP
        OBJECTS {
                    rpsuIndex, -- The number of RPSU
                    rpsuStatus
        }
        STATUS  current
        DESCRIPTION
           "These objects are required  to  control  traps."
       ::= { picaTrapGroups 1 }

    picaTrapEventGroup       NOTIFICATION-GROUP
        NOTIFICATIONS {
        switchFanFailed,
        switchFanPlugIn,
        switchFanPlugOut,
        switchFanRecovery,
        rpsuStateChange,
        rpsuPlugIn,
        rpsuPlugOut,
        rpsuFanFailed,
        rpsuStatusChangePowerOff,
        rpsuStatusChangePowerOn,
        rpsuFanRecovery,
        sfpPlugIn,
        sfpPlugOut,
        cpuHighThreshold,
        cpuLowThreshold,
        macThreshold
        }
    STATUS        current
    DESCRIPTION
     "A grouping of pica private trap events, as specified
     in NOTIFICATION-TYPE constructs."
    ::= { picaTrapGroups 2 }
```

```
END
```

Pica8 Public MIB

Download Pica8 supported publib MIBs here:

Supported Public MIBs.zip

The publib MIB SNMP-USER-BASED-SM-MIB is supported from PICOS 3.6.0, for details about this MIB, see http://net-snmp.sourceforge.net/docs/mibs/SNMP-USER-BASED-SM-MIB.txt.

SNMP Monitoring and Integration with Zabbix

Zabbix is an enterprise open-source monitoring solution for networking and applications. It is designed to monitor and track the status of various network services, servers, switches and other network hardware infrastructure.

SNMP can be used to monitor network devices in Zabbix. The Zabbix server uses SNMP OIDs for data collection, calculates triggers, and sends notifications to users on alerts.

We provide the following documents to guide the users to deploy PICOS SNMP with Zabbix.

1. PICOS Monitoring Solution Using Zabbix:

PICOS Monitoring Solution Using Zabbix.docx

2. **Zabbix Templates**:

zbx_SNMP_Linux_UCD-SNMPv3-MIB.xml

zbx_PICOS_Private_MIB.xml

PoE Configuration Guide

- Configuring PoE
- PoE over LLDP Power Negotiation
- UPoE
- Configuring Perpetual PoE

Configuring PoE

Introduction:

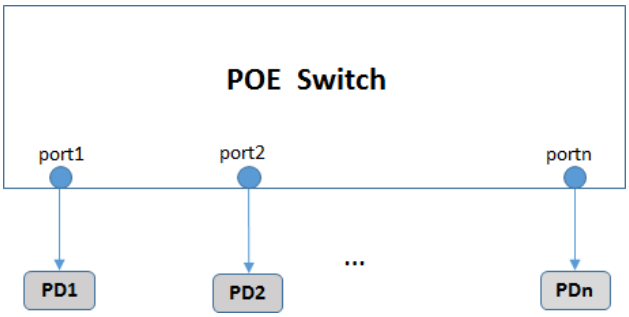
- Power over Ethernet(PoE) describes any of several standardized or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points and IP cameras.
- Power sourcing equipment (PSE) is a device such as a network Switch that provides (or sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE 802.3at, offers 25.50 W.
- A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP Cameras.

> ⚠ Only device models marked with P, PX, PXE, NPE, PE or EP support PoE. For FS switches, device models marked with P support PoE, device models marked with U support UPoE.

Topology:

Here is a typical topology for PoE. The PDs are power devices connected to a PoE switch.

Figure. Power devices(PD) connect with PoE switch



Configurations:

Enabling PoE on all ports is mandatory for other commands.

```
admin@XorPlus# set poe interface all enable true
admin@XorPlus# set poe interface all threshold-mode 2
admin@XorPlus# set poe interface all max-power 32
admin@XorPlus# set poe power management-mode 3
admin@XorPlus# set poe interface all mode signal
admin@XorPlus# set poe power mode redundant
admin@XorPlus# commit
```

For more details, please refer to PoE Configuration Commands.

PoE over LLDP Power Negotiation

- Introduction
  - Power via MDI TLV
  - PoE over LLDP Power Negotiation Mechanism
- Configuring PoE over LLDP Power Negotiation
  - Configuration Notes
  - Procedure
  - Configuration Example

Introduction

Power over Ethernet (PoE) enables electrical power to be carried over Ethernet cables, thus simplifying the deployment of networking equipment by eliminating the need for a power cord. Enabling it requires users to familiarize themselves with various PoE commands.

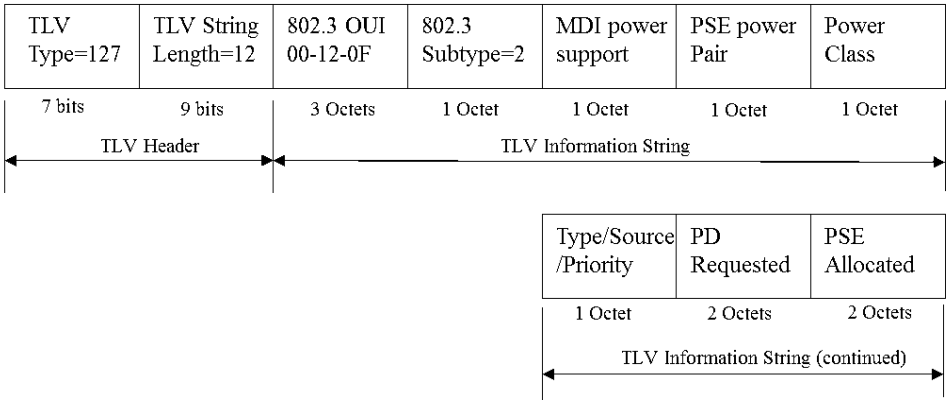
On this page, you will learn about one such PoE command, PoE over Link Layer Discovery Protocol (LLDP) power negotiation. This function allows a network switch, including an open white box switch, to assign the power priority value using LLDP to negotiate a power value, as opposed to using the power priority and value configured on the switch interface. The power negotiation process is described in detail, as is the switch configuration process.

Power via MDI TLV

IEEE 802.3 defines **Power via MDI TLV** to allow network management to advertise and discover power capability between LLDP-MED Endpoint and Network Connectivity Devices by sending LLDP negotiation packets.

The Power via MDI TLV is composed of 2-byte packet header and 12-byte TLV information field, as shown in Figure 1.

Figure 1. Power via MDI TLV packet format



The fields of Power via MDI TLV are described as follows:

- MDI power support

Field	Functions	Description
0	Port type	1: PSE-side port 0: PD-side port
1	Whether the PSE supports MDI power supply.	1: indicates that the PSE supports MDI power supply. 0: indicates that the PSE **does not** support MDI power supply.
2	MDI power supply status of the PSE.	1: enabled 0: disabled
3	Whether the PSE can control the line pair.	1: indicates that the PSE can control the line pair. 0: indicates that the PSE cannot control the line pair.
4-7	Reserved.	-

- PSE power Pair: The PSE power pair field contains an integer value as defined by the pethPsePortPowerPairs object in IETF RFC 3621.
- Power Class: The power class field contains an integer value as defined by the pethPsePortPowerClassifications object in IETF RFC 3621.
- Type/Source/Priority

Field	Functions	Description
Priority	Power supply priority of an interface.	11: indicates the lowest priority. 10: indicates the secondary highest priority. 01: indicates the highest priority. NOTE: This field contains four bits. The two left-most bits are reserved for the system.
Source	Power supply source.	PD: • 11: indicates the PSE and local source. • 10: indicates the local. • 01: indicates the PSE. PSE: • 11: indicates to be reserved. • 10: indicates the backup power supply. • 01: indicates the primary power supply.
Type	Power supply type.	01: indicates the PD that supports IEEE 802.3at. 00: indicates the PSE that supports IEEE 802.3at. 11: reserved. 10: reserved.

- PD Requested

Field	Functions	Value/Meaning
PD requested	PD requested power value	• Power=0.1*(decimal value of bits) Watts. The value is an integer that ranges from 1 to 255. For example, if the value of the field is 255, the exchange power is 25.5 W. • When the PoE power is sufficient, the values of PD Requested Power value and PSE allocated Power value are the same.

- PSE allocated

Field	Functions	Value/Meaning
PSE allocated	PSE allocated power value	• Power=0.1*(decimal value of bits) Watts. The value is an integer that ranges from 1 to 255. For example, if the value of the field is 255, the exchange power is 25.5 W. • When the PoE power is sufficient, the values of PD Requested Power value and PSE allocated Power value are the same.

PoE over LLDP Power Negotiation Mechanism

If PoE over LLDP power negotiation function is enabled on PSE, the PSE and the PD will periodically send LLDP packets to each other to perform LLDP power negotiation once the PD device is detected by the PSE. PoE over LLDP power negotiation starts when PSE receives LLDP packets from PD.

PoE over LLDP power negotiation message mechanism is as follows:

1. PD sends an LLDP packet to the PSE carries Power via MDI TLV, which contains the power supply priority of an interface and the PD requested power value.

2. PSE replies with an LLDP packet to the PD device. After receiving the LLDP packet from the PD device, the PSE allocates the corresponding power to the PD device and encapsulates it into the PSE allocated power value field in the Power via MDI TLV according to the PD requested value and its own power capabilities.

Configuring PoE over LLDP Power Negotiation

Configuration Notes

- All PoE devices support PoE over LLDP power negotiation function, except for S5810-48TS-P, S3410L-24TF-P, S5860-24XB-U,3410C-16TMS-P, 3410C-16TF-P and S3410C-8TMS-P.
- Enable LLDP function and PoE function before using PoE over LLDP power negotiation.
- When an expansion module is connected to the IP phone, in order to provide the required power to the expansion module, user should perform the following two operations to re-negotiate the PoE power supply.

  1). Enable the PoE over LLDP power negotiation function on the interface by using **set poe interface** <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**> command.

  2). Disable and re-enable PoE function of the interface by using **set poe interface {**<*port-id*> | **all} enable <true | false>** command.

Procedure

- Use the following command to disable or enable the PoE over LLDP power negotiation function.

set poe interface <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**>

By default, the function is enabled. To make the configuration take effect, user need to disable and re-enable PoE function of the interface by using **set poe interface {**<*port-id*> | **all} enable <true | false>** command.

Configuration Example

Networking Requirements

The networking requirements are as follows:

- An IP phone is connected to the Ge-1/1/1 port of the switch and an expansion module is connected to the IP phone.
- Enable PoE on port Ge-1/1/1 of the switch.
- When using PoE to power the IP phone, it also provides power for the expansion module which is connected to the IP phone. In this case, you need to enable the PoE over LLDP power negotiation function on the interface to assign the power priority and power value to the IP phone through LLDP power negotiation.

Procedure

Step1 Enable LLDP function.

```
admin@Xorplus# set protocols lldp enable true
```

Step2 Enable PoE function on interface Ge-1/1/1.

```
admin@XorPlus# set poe interface ge-1/1/1 enable true
```

Step3 Enable the PoE over LLDP power negotiation function on interface Ge-1/1/1.

```
admin@Xorplus# set poe interface ge-1/1/1 lldp-negotiation true
```

> When an expansion module is connected to the IP phone, in order to provide the required power to the expansion module, user should disable and re-enable PoE function of the interface by using **set poe interface {***<port-id>* | **all} enable <true | false>** command after enabled the PoE over LLDP power negotiation function.

Step4 Commit the configuration.

```
admin@Xorplus# commit
```

UPoE

With the development of technology, the maximum power required by the PD access devices has increased, and the maximum power provided by the PoE standard 802.3at cannot meet the power requirements. PICA8 supports the Universal Power over Ethernet (UPoE) function to provide more power to the PD devices, including IP cameras, video servers, compact switches and IP phones, etc. For details of UPoE support on each PoE platform, see set poe interface max-power.

You can use **set poe interface** {<*port-id*> | **all**} **max-power** <*integer*> command to set the maximum output power delivered by the PSE device.

Configuring Perpetual PoE

- Introduction
- Configuration Notes
- Configuring Perpetual PoE
  - Example

Introduction

Perpetual PoE (Power over Ethernet) is a feature that ensures continuous power supply to connected devices, even when the switch is rebooting. This capability is critical for maintaining uninterrupted operation of PoE-dependent devices such as IP cameras, VoIP phones, and wireless access points, ensuring they remain functional and avoid downtime during switch maintenance activities.

Configuration Notes

When configuring perpetual PoE, consider the following points:

- Only S5860-24XB-U switch supports perpetual PoE.
- Perpetual PoE supports maintaining uninterrupted power during a system reboot in the following scenarios.

  a. Execute the command **request system reboot** in L2/L3 CLI operating mode.

```
admin@PICOS> request system reboot
```

  b. Execute the **reboot** command in the Linux shell.

```
admin@PICOS:~$ sudo reboot
```

  c. Reboot during the upgrade process.

  d. For **nos-rollback** operation, if the version being rolled back to does not have Perpetual PoE configured, Perpetual PoE will not maintain uninterrupted power during the reboot in the NOS rollback process.

- Before restarting the S5860-24XB-U device, you need to save the configuration by executing **copy running-config startup-config** in L2/L3 CLI operating mode.
- Perpetual PoE will not maintain uninterrupted power in the following situations:

  a. Power failure or power cycling.

  b. PoE controller firmware update.

Configuring Perpetual PoE

- Use the following command to disable or enable the perpetual PoE function.

  set poe perpetual-power enable <**true** | **false**>

  By default, perpetual PoE is disabled.

Example

- This example shows how you can configure perpetual PoE on the switch.

```
admin@PICOS# set poe perpetual-power enable true
admin@PICOS# commit
```

Configuring USB Disable

Considering the system security, and in order to prevent the virus spreading through the USB interface, use USB disable function to disable external USB interface of the switch. All the external USB interfaces of the switch will be unavailable after they have been disabled.

Supported Platforms

The USB disable function is supported on the following platforms:

• AG9032

• 4806

• AS4610

• AS5712_54X

• AS5812_54X

• AS6712_32X

• AS7312_54X

• AS7712_32X

• S4048

• Z9100

Configuring USB Disable Function

Procedure

• Use the following command to disable or enable the USB interfaces of the switch.

set system usb disable [**true | false**]

The default setting is **set system usb disable false**. The command takes effect immediately after committing.

Configuration Example

• Disable the USB interfaces.

```
admin@Xorplus# set system usb disable true
admin@Xorplus# commit
```

• Enable the USB interfaces.

```
admin@Xorplus# set system usb disable false
admin@Xorplus# commit
```

Verify the Configuration

• Use **blkid** command to view the information of the switch disk. The external USB disk will not be shown if the USB interfaces are disabled.

```
 admin@Xorplus$blkid
/dev/sda1: LABEL="PicOS" UUID="4e223e38-59ca-40ca-93c0-7fc56afdf31b" TYPE="ext3"
/dev/sda2: LABEL="PICOS-BAK" UUID="f7908e2e-5054-4d6c-8d06-c227067dba01" SEC TYPE="ext2" TYPE="ext3"
```

Configuring CPU Usage Alarm Threshold

- Introduction
- Configuring CPU Usage Alarm Threshold
- Configuration Example
  - Procedure
  - Verify the Configuration

Introduction

The CPU is a core component of the device. When the system fails or suffers network attacks, it will take up a lot of CPU resources. This degrades system performance and results in data processing delays which in turn can potentially lead to high packet loss. During data processing, if the device can generate an SNMP Trap alarm when high CPU usage occurs, you can effectively monitor CPU usage and optimize system performance to maintain efficient data forwarding and network topology stability.

- CPU usage overload threshold and duration: When the CPU usage reaches the overload threshold with a continuous time, the system sends an SNMP Trap alarm message.
- CPU usage low threshold and duration: When the CPU usage falls below the low threshold for a continuous period of time, the system sends an SNMP Trap alarm message.

New PICA8 Private MIB Information

OID	Object Name	Description
1.3.6.1.4.1.35098.1.14.1.0	oidCpuThresholdStatus	This object is in configuration information node. The value of this object identifies whether the function of monitoring the switch CPU usage is enabled or disabled. The value could be 0 or 1. **0**: disable. **1**: enable.
1.3.6.1.4.1.35098.1.14.2.0	oidCpuHighThresholdValue	This object is in configuration information node. The value of this object identifies the overload threshold for CPU usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 80.
1.3.6.1.4.1.35098.1.14.3.0	oidCpuLowThresholdValue	This object is in configuration information node. The value of this object identifies the low threshold for CPU usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 20.
1.3.6.1.4.1.35098.1.14.4.0	oidCpuThresholdPeriod	This object is in configuration information node. The value of this object identifies the time duration when the CPU usage continues to exceed the overload threshold or fall below the low threshold. The value is an integer, in seconds, that ranges from 5 to 4294967295. The default value is 300s.
1.3.6.1.4.1.35098.21.4.1	oidCpuHighThreshold	This object is used in the syslog and SNMP Trap message, indicating the CPU usage reaches the overload threshold for a continuous period of time, the system sends an SNMP Trap alarm message.
1.3.6.1.4.1.35098.21.4.2	oidCpuLowThreshold	This object is used in the syslog and SNMP Trap message, indicating the CPU usage falls below the low threshold a continuous period of time, the system sends an SNMP Trap alarm message.

Configuring CPU Usage Alarm Threshold

Step1 Enable the function of monitoring the switch CPU usage.

set protocols snmp trap-group event cpu-threshold enable <**true** | **false**>

Step2 Set the overload threshold and low threshold for CPU usage monitoring to send SNMP Trap messages.

set protocols snmp trap-group event cpu-threshold high <*high-value*>

set protocols snmp trap-group event cpu-threshold low <*low-value*>

Step3 Configure the time duration for which the CPU usage continues to exceed the overload threshold or fall below the low threshold.

set protocols snmp trap-group event cpu-threshold interval <*interval*>

The system samples CPU usage one time every 5 seconds, if the CPU usage is out of the threshold range for this interval time, a SNMP trap message will be sent. But once CPU usage falls back into the threshold range and the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Configuration Example

Procedure

Step1 Configure the target host with IP address 10.10.50.16 for receiving SNMP traps.

```
admin@Xorplus#set protocols snmp community public
admin@Xorplus#set protocols snmp trap-group targets 10.10.50.16 security-name public
```

Step2 Enable the function of monitoring the switch CPU usage.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold enable true
```

Step3 Set the overload threshold and low threshold for CPU usage monitoring to send SNMP Trap messages.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold high 80
admin@Xorplus# set protocols snmp trap-group event cpu-threshold low 20
```

Step4 Configure the time duration for which the CPU usage continues to exceed the overload threshold or fall below the low threshold, and an SNMP Trap message will be sent.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold interval 300
```

Step5 Enable SNMP traceoptions for checking the SNMP syslog.

```
admin@Xorplus# set protocols snmp traceoptions flag all disable false
```

Step6 Commit the configuration.

```
admin@Xorplus# commit
```

Verify the Configuration

- User can check the syslogs when the CPU usage continuously exceeds the overload threshold or falls below the low threshold.

  Syslog message when the CPU usage monitoring continuously exceeds the overload threshold:

  2018-05-01 09:27:44.86 Xorplus local0.info : [SNMP]Trap: send v2 trap, community name public, oid: 1.3.6.1.4.1.35098.21.4.1, to:10.10.50.16/162

  Syslog message when the CPU usage monitoring continuously stays below the low threshold:

  2001-04-01 06:50:44.86 Xorplus local0.info : [SNMP]Trap: send v2 trap, community name public, oid: 1.3.6.1.4.1.35098.21.4.2, to:10.10.50.16/162

Configuring MAC Usage Alarm Threshold

- Introduction
- Configuring MAC address table usage Alarm Threshold
- Configuration Example
  - Procedure
  - Verify the Configuration

Introduction

MAC address table usage is an important indicator used to evaluate device performance. A high MAC address table usage will cause service faults. During data processing, if the device can generate an SNMP Trap alarm when high MAC address table usage occurs, you can effectively monitor MAC address table usage and optimize system performance to ensure system stability.

- MAC address table usage limit threshold and duration: When the MAC address table usage exceeds the limit threshold for a continuous period of time, the system sends an SNMP Trap alarm message.

New PICA8 Private MIB Information

OID	Object Name	Description
1.3.6.1.4.1.35098.1.15.1.0	oidMacThresholdStatus	This object is in configuration information node. The value of this object identifies whether the function of monitoring the switch MAC address table usage is enabled. The value could be 0 or 1. **0**: disable. **1**: enable.
1.3.6.1.4.1.35098.1.15.2.0	oidMacThresholdValue	This object is in configuration information node. The value of this object identifies the limit threshold for MAC address table usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 50.
1.3.6.1.4.1.35098.1.15.3.0	oidMacThresholdPeriod	This object is in configuration information node. The value of this object identifies the time duration when the MAC address table usage continues to exceed the limit threshold. The value is an integer, in seconds, that ranges from 5 to 4294967295. The default value is 300s.
1.3.6.1.4.1.35098.1.15.4.0	oidMacMonitorValue	This object is in configuration information node. The value of this object identifies the MAC address table usage when the system sends the last SNMP Trap message.
1.3.6.1.4.1.35098.21.5.1	oidMacThreshold	This object is used in the syslog and SNMP Trap message, indicating the MAC address table usage exceeds the limit threshold over a continuous time period. The system then sends an SNMP Trap alarm message.

Configuring MAC address table usage Alarm Threshold

Step1 Enable the function of monitoring the switch MAC address table usage.

set protocols snmp trap-group event mac-threshold enable <**true** | **false**>

Step2 Set the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

set protocols snmp trap-group event mac-threshold limit <*limit-value*>

Step3 Configure the time duration when the MAC address table usage continues to exceed the limit threshold.

set protocols snmp trap-group event mac-threshold interval <*interval*>

The system samples MAC address table usage one time every 10 seconds, if the MAC address table usage exceed the limit threshold over this interval time, a SNMP trap message will be sent. But once MAC address table usage falls back below the threshold when the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Configuration Example

Procedure

Step1 Configure the target host with IP address 10.10.50.16 for receiving SNMP traps.

```
admin@Xorplus#set protocols snmp community public
```

```
admin@Xorplus#set protocols snmp trap-group targets 10.10.50.16 security-name public
```

Step2 Enable the function of monitoring the switch MAC address table usage.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold enable true
```

Step3 Set the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold limit 50
```

Step4 Configure the time duration when the MAC address table usage continues to exceed the limit threshold, and an SNMP Trap message will be sent.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold interval 300
```

Step5 Enable SNMP traceoptions for checking the SNMP syslogs.

```
admin@Xorplus# set protocols snmp traceoptions flag all disable false
```

Step6 Commit the configuration.

```
admin@Xorplus# commit
```

Verify the Configuration

- User can check the syslog when the MAC address table usage monitoring continuously exceeds the limit threshold.

  2001-01-01 06:27:44.86 Xorplus local0.info : [SNMP]Trap: send v2 trap, community name public, oid: 1.3.6.1.4.1.35098.21.5.1, to:10.10.50.16/162

Mirror Configuration

- Introduction of Mirroring
- Configuration Notes of Mirroring
- Configuring Mirror
- Example for Configuring Local Port Mirroring
- Example for Configuring ERSPAN
- Example for Configuring ACL-based ERSPAN

Introduction of Mirroring

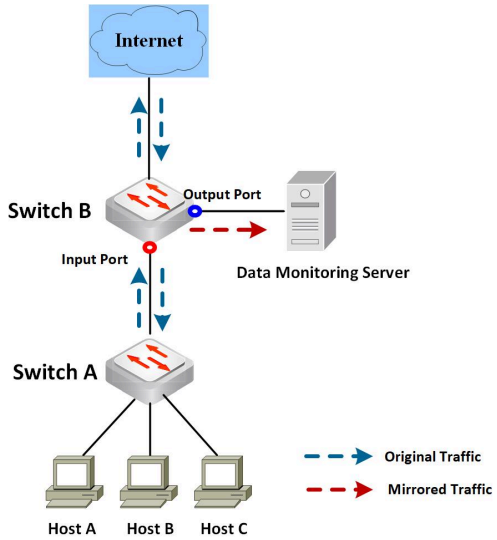
- Local Port Mirroring
- Remote Port Mirroring
  - ERSPAN
  - ACL-based ERSPAN

PICOS port mirroring supports two scenarios: local port mirroring and remote port mirroring.

Local Port Mirroring

In local port mirroring, the output port is directly connected to the Data Monitoring Server. As shown in **Figure 1**, local port mirroring is enabled on Switch B, the output port forwards the messages copied from the input port to the data monitoring server directly connected to it.

Figure1. Local Port Mirroring



NOTEs:

- The mirroring port can belong to any VLAN. This port can be either a trunk port or an access port but will not participate in Layer2 or Layer3 forwarding.
- The egress port or ingress port can be either an access port or a trunk port.
- When user sends untagged packets, the priority of mirroring is higher than the priority of adding tag.
- When user receives tagged packets, the priority of mirroring is higher than the priority of removing tag.
- The mirroring port can also analyze BPDU/LACP/LLDP packets.
- When user configures ACL for ingress/egress port, the priority of mirroring is higher than the priority of filter.
- The duplicated traffic of egress port may be different from the outgoing traffic as there are other forwarding operations before or after the mirroring operation. For example, if the received packet is tagged with PVID, the PVID tag needs to be stripped off before forwarding the packet, the duplicated traffic may be different from the outgoing traffic because it may have been duplicated to the mirroring port before the PVID was stripped off.

On the following platforms, the duplicate packets are the same as the outgoing packets, but it is not certain on other platforms.

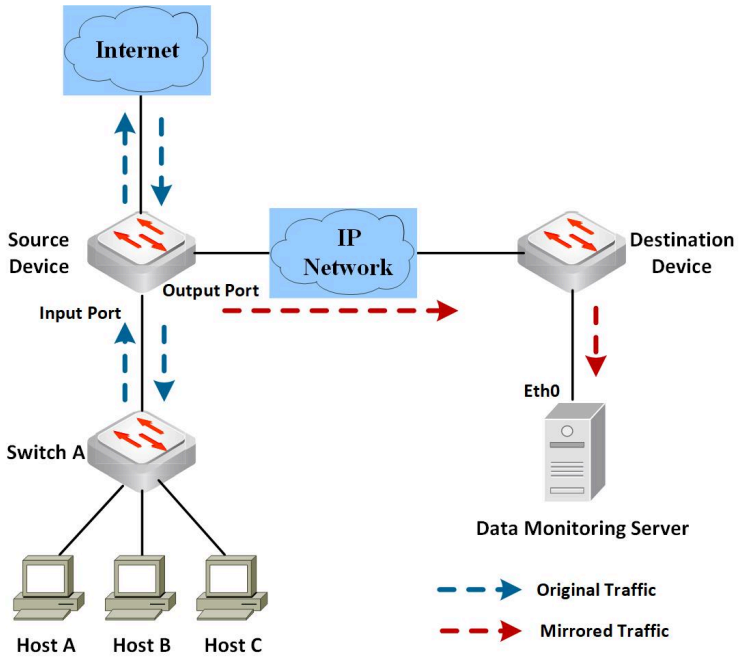
Switch ASIC	Model
Triumph2	PRONTO3296, PRONTO3295, PRONTO3290
Appllo2	ES4654
Helix4	AS4610 Series Switches

Remote Port Mirroring

ERSPAN

As shown in **Figure 2**, ERSPAN (Encapsulated Remote Switched Port Analyzer) is a remote port mirroring technology which is enabled on the mirror Source Device. In ERSPAN, the output port remotely connects to the Data Monitoring Server, and forwards the copied message from the input port to the Data Monitoring Server through a GRE tunnel over the IP network.

Figure 2. ERSPAN (Encapsulated Remote Switched Port Analyzer)



The output port encapsulates the original mirrored layer 2 packet with the GRE tunnel header, and then sends the entire GRE message in the data part of the IP message through the GRE tunnel. The encapsulated packets have the following format:

| MAC_HEADER | IP_HEADER | GRE_HEADER | L2_Mirrored_Packet |

The IP header encapsulated in the outer layer of the GRE message is manually configured by the following commands:

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output source-ip** <*source-ip*>

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output dest-ip** <*dest-ip*>

After configuration, use command **run show analyzer** [<*mirror-name*>] to display information about the mirroring information.

The switch finds the outgoing port of the mirror packet by looking for the destination IP network in its routing table. When configuring, the specified destination IP address should be configured the same as the IP address of the remote Data Monitoring Server to ensure the destination is reachable for the mirrored messages. Usually, the source IP address can be configured as the IP address of the Source Device.

As shown in **Figure 2**, the Source Device is not required to support the GRE function. ERSPAN is provided with GRE tunnel encapsulation capability. As a route forwarding device, Destination Device forwards GRE messages to the Data Monitoring Server.

The Data Monitoring Server does not need to support ERSPAN, but should support Linux GRE to decapsulate the receiving GRE messages.

NOTEs:

- A pair of source IP and destination IP addresses form a GRE tunnel.
- Multiple input ports mirroring through the same GRE tunnel is allowed only when the analyzer names are the same. However, the same GRE tunnel cannot be configured to different analyzer names, or it will commit fail and an error will be printed: "**the same erspan tunnel already exists**". For example,

```
admin@Xorplus# set interface ethernet-switching-options analyzer 333 erspan input egress te-1/1/2
admin@Xorplus# set interface ethernet-switching-options analyzer 333 erspan output source-ip 100.100.100.100
admin@Xorplus# commit
admin@Xorplus# set interface ethernet-switching-options analyzer 444 erspan input ingress te-1/1/1
admin@Xorplus# set interface ethernet-switching-options analyzer 444 erspan output source-ip 100.100.100.100
admin@Xorplus# set interface ethernet-switching-options analyzer 444 erspan output dest-ip 200.200.200.200
admin@Xorplus# commit
the same erspan tunnel already exist
Commit failed.
```

ACL-based ERSPAN

In ACL-based ERSPAN, service flows matching configured ACL rules is copied to the mirroring output port and then forwarded to the remote monitoring device through the GRE tunnel for analysis and monitoring. As shown in **Figure 2** in last section, on the Source Device, the input port copies the service flows matching the ACL rules to the output port, and then the output port forwards the copied service flows through the GRE tunnel to the remote monitoring device.

ACL-based ERSPAN is a remote port mirroring feature developed based on PICOS firewall filter feature, which supports all the firewall filter matching fields (*destination-address-ipv4, destination-mac-address, destination-port, ospf, etc.*) except the IPv6 filters (*destination-address-ipv6/ source-address-ipv6).*

Security ACL filter rules and ACL-based ERSPAN rules are put together in the order of the sequence number, which is also the match priority. The match criteria of ACL-based ERSPAN rules is the same as that of Security ACL rules, please refer to ACL configuration guide for details about Security ACL.

The ACL action commands of ACL-based ERSPAN are listed below, which are separated from the Security ACL action:

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan source-ip** <*source-ip*>

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan dest-ip** <*dest-ip*>

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan vrf** <*vrf-name*>

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan ttl** <*ttl-value*>

After configuration, use command **run show filter** [<*text*>] to display information about all filters or a specified filter.

Configuration Notes of Mirroring

- A device can be configured with up to four mirror analyzer names, including both local port mirroring and remote port mirroring.
- For local port mirroring, multiple input ports mirroring to the same output port is allowed only when the analyzer names are the same. However, multiple input ports mirroring to the same output port is not supported when analyzer names are different.
- For local port mirroring, the output port cannot participate in Layer 2 or Layer 3 forwarding.
- ERSPAN/ACL-based ERSPAN does not support IPv6.
- Due to hardware restrictions, currently it only supports to apply the ACL rules to the ingress direction of the mirroring input port.
- ERSPAN does not support BGP unnumbered routing and leaked route. The run show analyzer command, the mirror "state" is displayed as *Down* in these scenarios.
- ERSPAN does not support that the output port and input port are the same port.
- The ERSPAN output port cannot be a LAG port.

Configuring Mirror

- Configuring Local Port Mirroring
- Configuring ERSPAN
  - ERSPAN Configurations on the Source Device
- Configuring ACL-based ERSPAN

Configuring Local Port Mirroring

Step 1 Configure the input port for mirror.

set interface ethernet-switching-options analyzer <*mirror-name*> **input ingress** <*port-name*>

set interface ethernet-switching-options analyzer <*mirror-name*> **input egress** <*port-name*>

Step 2 Configure the output port for mirror.

set interface ethernet-switching-options analyzer <*mirror-name*> **output** <*port-name*>

Step 3 Commit the configurations.

commit

Step 4 Verify the configuration.

run show analyzer [<*mirror-name*>]

Configuring ERSPAN

In addition to the following ERSPAN configurations on the source device, you have to complete two extra configurations on the route device and remote data monitoring server. For details, please refer to Example for Configuring ERSPAN.

- The remote data monitoring server does not need to support ERSPAN, but should support Linux GRE to decapsulate the receiving GRE message.
- Configure routing protocols on all routing devices to ensure the mirroring source device and the data monitoring server route reachable.

ERSPAN Configurations on the Source Device

Step 1 Configure the input port for ERSPAN mirror.

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input ingress**<*port-name*>

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input egress**<*port-name*>

Step 2 Configure the source IP address and destination IP address for ERSPAN encapsulation.

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output source-ip** <*source-ip*>

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output dest-ip** <*dest-ip*>

Step 3 Enable IP routing for L3 forwarding.

set ip routing enable <**true|false**>

Step 4 Commit the configurations.

commit

Step 5 Verify the configuration.

run show analyzer [<*mirror-name*>]

Configuring ACL-based ERSPAN

Step 1 Configure ACL filter rules. You can refer to ACL configuration guide for details about how to configure ACL filter rules.

set firewall filter <*filter-name*> **sequence** <*number*> **from** *XX*

Step 2 Apply the ACL filter rules to the mirroring input port.

NOTE: Due to hardware restrictions, currently it only supports to apply the ACL rules to the ingress direction of the mirroring input port. That is, the command **set firewall filter** <*filter-name*> **output interface** <*interface-name*> does not support for ACL-based ERSPAN.

set firewall filter <*filter-name*> **input interface** <*interface-name*>

Step 3 Configure the source IP address and destination IP address for ACL-based ERSPAN GRE

NOTE: The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan source-ip** <*source-ip*>

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan dest-ip** <*dest-ip*>

Step 4 Enable IP routing for L3 forwarding.

set ip routing enable <**true|false**>

Step 5 Commit the configurations.

commit

Step 6 Verify the configuration.

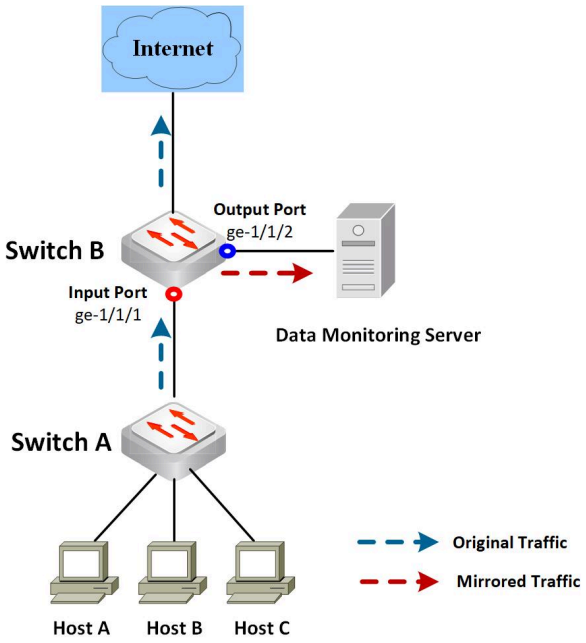
run show filter [*<filter-name>*]

Example for Configuring Local Port Mirroring

- Networking Requirements
- Procedure

Networking Requirements

Figure 1. Local Port Mirroring Configuration Example



As shown in **Figure 1**, Host A, Host B and Host C access the Internet through Switch B. The Data Monitoring Server needs to monitor the traffic from the three hosts accessing the internet.

Follow the following configuration procedure on Switch B to complete port mirroring configurations to achieve above requirement.

1. Configure interface ge-1/1/2 as the output port for mirroring, which is responsible for forwarding mirrored messages to the Data Monitoring Server.
2. Configure interface ge-1/1/1 as the input port for mirroring to make a copy of the traffic from Host A, Host B and Host C accessing the Internet to the mirroring output port.

Procedure

Step 1 Configure VLAN.

```
admin@SwitchB# set vlans vlan-id 110
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 110
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 110
```

Step 2 Configure the input port for mirroring.

```
admin@SwitchB# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/1
admin@SwitchB# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/1
```

Step 3 Configure the output port for mirroring.

```
admin@SwitchB# set interface ethernet-switching-options analyzer 111 output ge-1/1/2
```

Step 4 Commit the configurations.

```
admin@SwitchB# commit
```

Step 5 Verify the configuration.

```
admin@SwitchB# run show analyzer 111
```

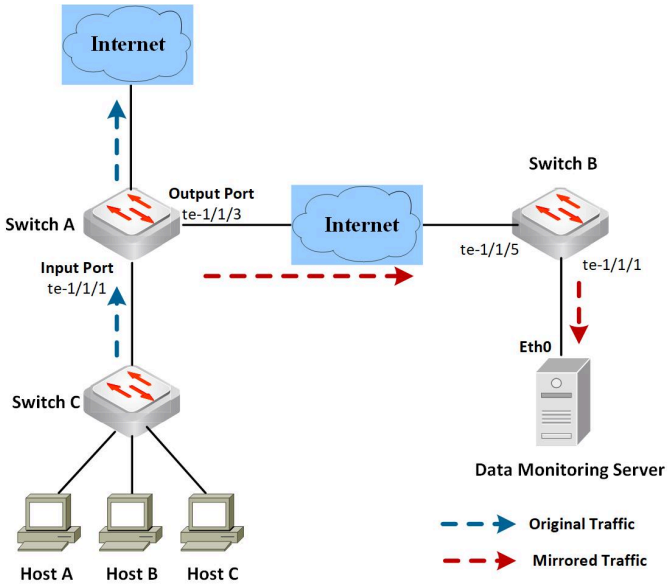
```
Analyzer name: 111
Output interface: <ge-1/1/2>
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces: <ge-1/1/1>
```

Example for Configuring ERSPAN

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Data Monitoring Server
  - Host
- Verify Configuration

Networking Requirements

Figure 1. ERSPAN Configuration Example



As shown in **Figure 1**, Host A, Host B and Host C access the Internet through Switch A. The remote Data Monitoring Server connects to Switch A through Switch B. To monitor the traffic from the three hosts, the data needs to be mirrored to the output port and carried across the tunnel to the remote Data Monitoring Server.

Follow the configuration steps listed below to enable the remote port mirroring function:

1. Configure interface te-1/1/3 on Switch A as the output port for ERSPAN mirroring, which is responsible for forwarding mirrored messages to Switch B through GRE tunnel.
2. Configure interface te-1/1/1 on Switch A as the input port for ERSPAN mirroring to copy the traffic from Host A, Host B and Host C accessing the Internet to the output port.
3. On Switch B, create the VLAN and VLAN interface for forwarding mirrored messages to the Data Monitoring Server.
4. On Data Monitoring Server, configure Linux GRE to decapsulate the receiving GRE messages.

Procedure

Switch A

Step 1 Configure VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 100
admin@SwitchA# set vlans vlan-id 230
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 230
admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchA# set vlans vlan-id 230 l3-interface vlan230
admin@SwitchA# set l3-interface vlan-interface vlan100 address 100.100.100.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan230 address 220.220.220.1 prefix-length 24
```

Step 2 Configure the input port for ERSPAN mirror.

```
admin@SwitchA# set interface ethernet-switching-options analyzer 112 erspan input ingress te-1/1/1
```

Step 3 Configure the source IP address and destination IP address for ERSPAN encapsulation.

```
admin@SwitchA# set interface ethernet-switching-options analyzer 112 erspan output source-ip 4.4.4.4
admin@SwitchA# set interface ethernet-switching-options analyzer 112 erspan output dest-ip 8.8.8.8
```

Step 4 Configure routing protocol and enable IP routing for L3 forwarding.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf area 0
admin@SwitchA# set protocols ospf network 100.100.100.0/24 area 0
admin@SwitchA# set protocols ospf network 220.220.220.0/24 area 0
admin@SwitchA# set ip routing enable true
```

Step 5 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step 1 Configure VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 100
admin@SwitchB# set vlans vlan-id 230
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 230
admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchB# set vlans vlan-id 230 l3-interface vlan230
admin@SwitchB# set l3-interface vlan-interface vlan100 address 8.8.8.1 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan230 address 220.220.220.2 prefix-length 24
```

Step 2 Configure routing protocol and enable IP routing for L3 forwarding.

```
admin@SwitchB# set protocols ospf router-id 3.3.3.3
admin@SwitchB# set protocols ospf area 0
admin@SwitchB# set protocols ospf network 220.220.220.0/24 area 0
admin@SwitchB# set protocols ospf network 8.8.8.0/24 area 0
admin@SwitchB# set ip routing enable true
```

Step 3 Commit the configurations.

```
admin@SwitchB# commit
```

Data Monitoring Server

On the Data Monitoring Server, configure Linux GRE to decapsulate the receiving GRE messages on Linux shell.

```
root@Monitoring_Server:/home/admin# ip addr add 8.8.8.8/24 dev eth0
root@Monitoring_Server:/home/admin# ip link add mm type erspan local 8.8.8.8 erspan_ver 0
root@Monitoring_Server:/home/admin# ip link set mm up
```

Host

No configuration is necessary on the hosts. Any packet the hosts send which flows through Switch A will automatically be copied across the ERSPAN tunnel to the Data Monitoring Server.

Verify Configuration

- On Switch A, run command **run show analyzer** to view the mirroring information.

```
admin@SwitchA# run show analyzer 112
Analyzer name: 112
Erspan Output:
       state: UP
       source-ip: 4.4.4.4
       dest-ip: 8.8.8.8
       output-port: te-1/1/3
       tagged vlan:
```

```
       vrf:
Ingress monitored interfaces: <te-1/1/1>
Egress monitored interfaces:
```

- The Data Monitoring Server can normally receive the mirrored message.
  - Check the received mirrored message.

```
root@ Monitoring_Server:/home/admin# tcpdump -i eth0 -net -vv
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
cc:37:ab:f4:81:95 > 70:72:cf:b7:65:44, ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 254, id 0, offset 0, flags [none], proto GRE (47), length 84)
    4.4.4.4 > 8.8.8.8: GREv0, Flags [none], proto unknown (0x88be), length 64
        gre-proto-0x88be
cc:37:ab:f4:81:95 > 70:72:cf:b7:65:44, ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 254, id 0, offset 0, flags [none], proto GRE (47), length 84)
    4.4.4.4 > 8.8.8.8: GREv0, Flags [none], proto unknown (0x88be), length 64
        gre-proto-0x88be
cc:37:ab:f4:81:95 > 70:72:cf:b7:65:44, ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 254, id 0, offset 0, flags [none], proto GRE (47), length 84)
    4.4.4.4 > 8.8.8.8: GREv0, Flags [none], proto unknown (0x88be), length 64
        gre-proto-0x88be
```

- View the decapsulated mirrored message.

```
root@ Monitoring_Server:/home/admin# tcpdump -i mm -net -vv
```

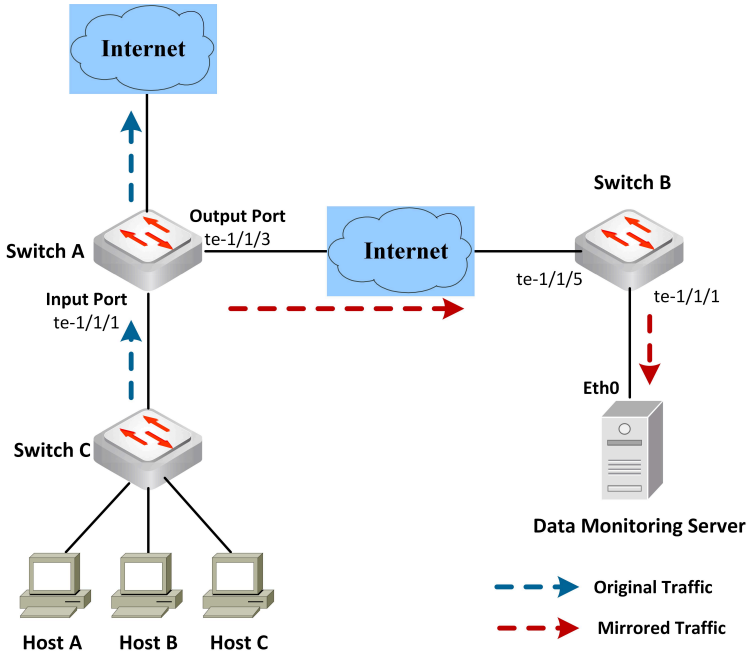
```
tcpdump: listening on mm, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
22:11:11:11:11:11 > 66:66:66:66:66:66, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 64, id 0, offset 0, flags [none], proto TCP (6), length 46)
    1.1.1.2.0 > 5.5.5.100.0: Flags [none], cksum 0x9d6a (correct), seq 0:6, win 0, length 6
```

Example for Configuring ACL-based ERSPAN

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Data Monitoring Server
  - Host
- Verify Configuration

Networking Requirements

Figure 1. ACL-based ERSPAN Configuration Example



As shown in **Figure 1**, Host A, Host B and Host C access the Internet through Switch A. The remote Data Monitoring Server connects to Switch A through Switch B. To monitor the traffic from the three hosts, the data needs to be mirrored to the output port and carried across the tunnel to the remote Data Monitoring Server. The network administrator hopes that the Data Monitoring Server can analyze the packet flow matching both the TCP protocol and the source IPv4 address of 1.1.1.0/24 network segment, so as to locate the source of malicious attack.

Follow the configuration steps listed below to enable the ACL-based ERSPAN function:

1. On Switch A, configure ACL filter rules for ACL-based ERSPAN and apply the ACL rules to the mirroring input port te-1/1/1.
2. On Switch A, configure the source IP address and destination IP address for ACL-based ERSPAN GRE encapsulation.
3. On Switch B, create the VLAN and VLAN interface for forwarding mirrored messages to the Data Monitoring Server.
4. On Data Monitoring Server, configure Linux GRE to decapsulate the receiving GRE messages.

Procedure

Switch A

Step 1 Configure VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 100
admin@SwitchA# set vlans vlan-id 230
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 230
admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchA# set vlans vlan-id 230 l3-interface vlan230
admin@SwitchA# set l3-interface vlan-interface vlan100 address 100.100.100.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan230 address 220.220.220.1 prefix-length 24
```

Step 2 Configure ACL filter rules. You can refer to ACL configuration guide for details about how to configure ACL filter rules.

```
admin@SwitchA# set firewall filter f1 sequence 1 from protocol tcp
admin@SwitchA# set firewall filter f1 sequence 1 from source-address-ipv4 1.1.1.0/24
```

Step 3 Apply the ACL filter rules to the mirroring input port.

NOTE: Due to hardware restrictions, currently it only supports to apply the ACL rules to the ingress direction of the mirroring input port. That is, the command **set firewall filter** <*filter-name*> **output interface** <*interface-name*> does not support for ACL-based ERSPAN.

```
admin@SwitchA# set firewall filter f1 input interface te-1/1/1
```

Step 3 Configure the source IP address and destination IP address for ACL-based ERSPAN encapsulation.

```
admin@SwitchA# set firewall filter f1 sequence 1 then erspan source-ip 4.4.4.4
admin@SwitchA# set firewall filter f1 sequence 1 then erspan dest-ip 8.8.8.8
```

Step 4 Configure routing protocol and enable IP routing for L3 forwarding.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf area 0
admin@SwitchA# set protocols ospf network 100.100.100.0/24 area 0
admin@SwitchA# set protocols ospf network 220.220.220.0/24 area 0
admin@SwitchA# set ip routing enable true
```

Step 5 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step 1 Configure VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 100
admin@SwitchB# set vlans vlan-id 230
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 230
admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchB# set vlans vlan-id 230 l3-interface vlan230
admin@SwitchB# set l3-interface vlan-interface vlan100 address 8.8.8.1 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan230 address 220.220.220.2 prefix-length 24
```

Step 2 Configure routing protocol and enable IP routing for L3 forwarding.

```
admin@SwitchB# set protocols ospf router-id 3.3.3.3
admin@SwitchB# set protocols ospf area 0
admin@SwitchB# set protocols ospf network 220.220.220.0/24 area 0
admin@SwitchB# set protocols ospf network 8.8.8.0/24 area 0
admin@SwitchB# set ip routing enable true
```

Step 3 Commit the configurations.

```
admin@SwitchB# commit
```

Data Monitoring Server

On the Data Monitoring Server, configure Linux GRE to decapsulate the receiving GRE messages on Linux shell.

```
root@Monitoring_Server:/home/admin# ip addr add 8.8.8.8/24 dev eth0
root@Monitoring_Server:/home/admin# ip link add mm type erspan local 8.8.8.8 erspan_ver 0
root@Monitoring_Server:/home/admin# ip link set mm up
```

Host

No configuration is necessary on the hosts. Any packet the hosts send which flows through Switch A will automatically be copied across the ERSPAN tunnel to the Data Monitoring Server.

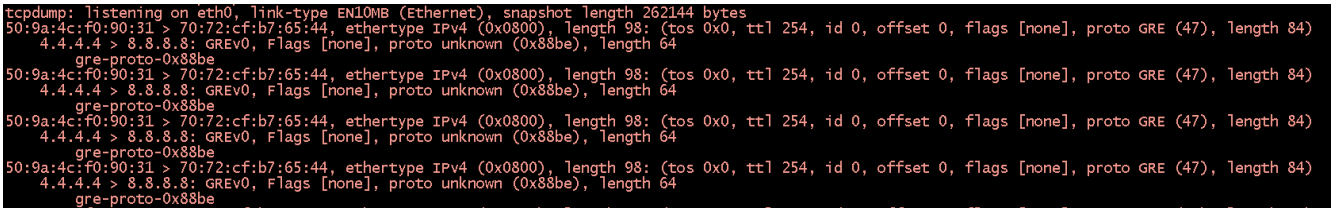
Verify Configuration

- On Switch A, run command **run show filter** to view the configuration information about ACL-based ERSPAN.

```
admin@SwitchA# run show filter f1
Filter: f1
    Description:
    Sequence: 1
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                tcp
            source-address-ipv4:     1.1.1.0/24
        action: forward
        Erspan Output:
               state: UP
               source-ip: 4.4.4.4
               dest-ip: 8.8.8.8
               output-port: te-1/1/3
               tagged vlan:
               vrf:
               ttl: 255
        forwarding_class:
Input interface: te-1/1/1
```

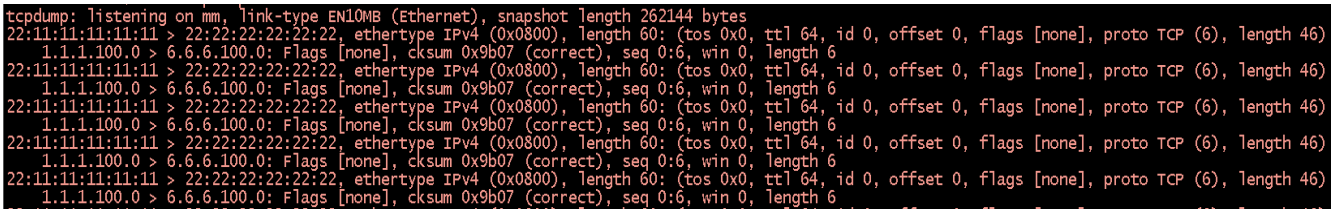
- The Data Monitoring Server can normally receive the mirrored message.
  - Check the received mirrored message.

```
root@Monitoring_Server:/home/admin# tcpdump -i eth0 -net -vv
```



  - View the decapsulated mirrored message.

```
root@Monitoring_Server:/home/admin# tcpdump -i mm -net -vv
```

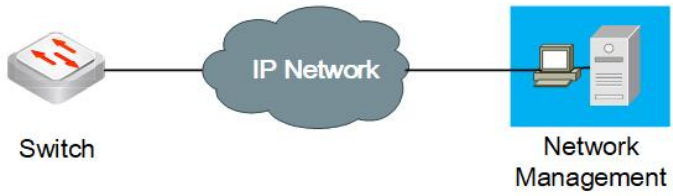


Configuring gNMI-gRPC Based Telemetry Technology

Overview

Telemetry is a remote data collection technology for monitoring device performance and faults. Telemetry technology uses the gRPC protocol to push data from the network device to a collector in the network management system. As shown in Figure 1, after a gRPC connection is established between the switch and the network management system, the network manager can subscribe to the data information of the specified service module on the switch.

Figure 1. gNMI-gRPC-based Telemetry Technology



PICOS currently only supports dial-in mode of Telemetry technology. In dial-in mode, the switch acts as a gRPC server and the collector acts as a gRPC client. The collector initiates a gRPC connection to the switch and subscribes to the data that needs to be collected.

PICOS Telemetry technology supports **Get** and **Subscribe** operations based on gNMI (gRPC Network Management Interface):

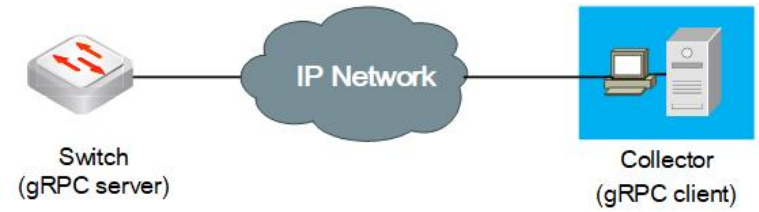
- **gNMI Get operation**: Get the device operating status and operating configuration.
- **gNMI Subscribe operation**: Subscribe to the data push service to the device, including event-triggered data and periodically sampled data.

gNMI uses gRPC (Google Remote Procedure Call) as its transport protocol.

Configuration Example for gRPC Dial-in Mode

Networking Requirements

Figure 2. gRPC Dial-in Mode Configuration Group Diagram



As shown in Figure 2, the Switch is connected to the Collector as a gRPC server. The Collector is the gRPC client. By configuring gRPC dial-in mode on the Switch, the Collector can subscribe to LLDP events on the Switch.

Configuring the gRPC Server

Before configuring the gRPC server, it is assumed that the IP addresses of both the gRPC server and the gRPC client are properly configured so that the two have valid routes to reach one another. Also make sure the gRPC environment is installed on the gRPC client.

Step 1 Enable gRPC function.

```
admin@XorPlus# set protocols grpc enable true
```

Step 2 (Optional) Configure the listening port number.

```
admin@XorPlus# set protocols grpc port 10500
```

Step 3 Commit the configuration.

```
admin@XorPlus# commit
```

Verify the Configuration

When an LLDP event occurs on the Switch, the gRPC client successfully receives the subscription information on the switch.

Remote Network Monitoring (RMON)

- Overview of RMON
- Configuring RMON
- Example for Configuring RMON

Overview of RMON

RMON is implemented based on the SNMP architecture and shares a set of Network Management Station (NMS) with SNMP to remotely manage devices.

The RMON standard (RFC2819) defines multiple RMON groups, and the device implements the four groups supported in public MIBs: statistics, history, alarms, and events, achieving the following four statistics and alarm functions for remote monitoring and management of devices in the network.

- **Ethernet statistics function (etherStatsTable in RMON MIB):** the basic statistics of each network being monitored. The system continuously gathers statistics for the traffic and the distribution of various types of packets like broadcast and multicast, the number of collisions, the number of CRC checksum error messages, the number of undersized (or oversized) data messages, and the number of received bytes and dropped packets.
- **History statistics function (etherHistoryTable in RMON MIB):** The system periodically samples, collects and stores the network statistics information. The statistics include bandwidth utilization, number of error packets and total packets, etc.
- **Event definition function (eventTable and logTable in RMON MIB):** The event group controls the events and prompts coming from the device, providing information about all events generated by RMON agent. When an event occurs, a log can be recorded or a trap can be sent to the network management station.
- **Alarm threshold setting function (alarmTable in RMON MIB):** The system monitors the specified alarm variable (alarm object corresponding to the SNMP OID). The RMON agent will record the monitored status as a log or send the trap to the network management station.

Configuring RMON

Downloading RMON MIB

Users can download RMON MIB from the page Pica8 Public MIB.

Configuring RMON

The RMON configuration contains two parts: RMON statistics and RMON alarm.

Configuring RMON Statistics

RMON statistics contains RMON ethernet statistics and history statistics:

- RMON Ethernet statistics monitors traffic with continuous statistics on the Ethernet interface. It counts the number of broadcast and multicast messages, the number of network conflicts, the number of CRC checksum error messages, the number of undersized (or oversized) data messages, the number of dropped messages, and the number of received packets in bytes.
- Configure RMON historical statistics function when you want to periodically collect data on a specified interface. It gathers statistics for the bandwidth utilization, the number of error packets, the total number of packets, etc.

Configuring RMON Ethernet Statistics

Step1 Configure RMON ethernet statistics on a specified interface.

set protocols snmp rmon statistics <*entry-index*> **interface** <*interface-name*>

Step2 Configure the owner's name of the RMON ethernet statistics table.

set protocols snmp rmon statistics <*entry-index*> **owner** <*string*>

Step3 Commit after completing all the above configurations.

commit

Step4 View RMON Ethernet statistics information.

run show rmon statistics [<*entry-index*>]

Configuring RMON History Statistics

Step1 Configure RMON history statistics on a specified interface.

set protocols snmp rmon history <*entry-index*> **interface** <*interface-name*>

Step2 Configure the sampling interval of RMON history statistics.

set protocols snmp rmon history <*entry-index*> **interval** <*interval*>

Step3 Configure the history statistics table capacity, that is, the maximum number of records that the history table can hold.

set protocols snmp rmon history <*entry-index*> **buckets** <*number*>

Step4 Configure the owner's name of the RMON history statistics table.

set protocols snmp rmon history <*entry-index*> **owner** <*string*>

Step5 Commit after completing all the above configurations.

commit

Step6 View RMON history statistics information.

run show rmon history [<*entry-index*>]

Configuring RMON Alarm

To configure RMON alarm function, users need to configure both RMON event definition function and RMON alarm threshold setting function. The RMON alarm threshold setting function configures the monitoring object and threshold. The RMON event definition function defines the action whether to record a log

or send a trap information to the NMS when a RMON alarm event triggered.

Configuring RMON Event

Step1 Configure the community for the RMON event.

set protocols snmp rmon event <*entry-index*> **community** <*community*>

Step2 Configure the RMON event action type.

set protocols snmp rmon event <*entry-index*> **type** <**none** | **log** | **trap** | **log-trap**>

Step3 Enable SNMP trap. If the event is triggered and the event action type is **trap** or **log- trap**, an SNMP trap will be sent to the management station. The value of **community** and **security-name** here should be the same as the **community** in step 1.

set protocols snmp community <*community*>

set protocols snmp trap-group targets <*ip_address*> **security-name** <*security-name*>

Step4 Configure the description for the RMON event.

set protocols snmp rmon event <*entry-index*> **description** <*event_description*>

Step5 Configure the owner's name of the RMON event.

set protocols snmp rmon event <*entry-index*> **owner** <*owner*>

Step6 Commit after completing all the above configurations.

commit

Step7 View RMON event and event log information.

run show rmon events [<*entry-index*>]

run show rmon eventlog [<*entry-index*>]

Configuring RMON Alarm

Step1 Configure the OID of the RMON alarm.

set protocols snmp rmon alarm <*entry-index*> **variable** <*oid-variable*>

Step2 Configure the sampling type of RMON alarm.

set protocols snmp rmon alarm <*entry-index*> **sample-type** <**absolute** | **delta**>

Step3 Configure the sampling interval of RMON alarm.

set protocols snmp rmon alarm <*entry-index*> **interval** <*interval*>

Step4 Configure the rising threshold of the RMON alarm, and the event to fire when the rising threshold is crossed.

set protocols snmp rmon alarm <*entry-index*> **rising-threshold** <*alarmRisingThreshold*>

set protocols snmp rmon alarm <*entry-index*> **rising-event-index** <*alarmRisingEventIndex*>

Step5 Configure the falling threshold of the RMON alarm, and the event to fire when the falling threshold is crossed.

set protocols snmp rmon alarm <*entry-index*> **falling-threshold** <*alarmFallingThreshold*>

set protocols snmp rmon alarm <*entry-index*> **falling-event-index** <*alarmFallingEventIndex*>

Step6 Configure the owner's name of the RMON alarm.

set protocols snmp rmon alarm <*entry-index*> **owner** <*owner*>

Step7 Commit after completing all the above configurations.

commit

Step8 View RMON alarms information.

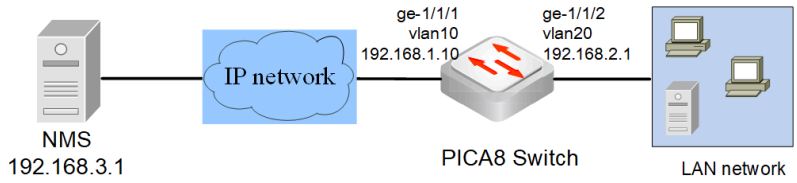
run show rmon alarms [<*entry-index*>]

Example for Configuring RMON

- Networking Requirements
  - Configuration Roadmap
- Procedure
- Verifying the Configuration

Networking Requirements

Figure 1. RMON Configuration Example



As shown in **Figure 1**, to monitor the LAN network connected to PICA8 Switch's interface ge-1/1/1, RMON is enabled to achieve the following requirement:

- Real-time and historical statistical information on traffic and the number of various types of packets.
- Record a log when the flow rate per minute (MIB variable 1.3.6.1.2.1.16.1.1.1.4.1) exceeds the set threshold.
- Monitor the broadcast and multicast traffic of this LAN subnet and report alarm messages to the NMS when exceeding the set threshold.

Configuration Roadmap

The RMON statistics function can be configured on PICA8 Switch to monitor real-time and history statistics of traffic and the number of various types of packets. Configuring RMON alarm function can record the log and actively report alarm information to NMS when the traffic exceeds the set threshold.

1. Configure the IP address of the switch interface and route reachability on the network.
2. Configure to allow Trap messages to be sent to the NMS.
3. Enable the RMON ethernet statistics and history statistics function.
4. Configure both RMON event definition function and alarm threshold setting function to achieve RMON alarm function.

Procedure

Step1 Configure the IP address of the switch interface.

```
admin@Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@Switch# set vlans vlan-id 10 l3-interface vlan10
admin@Switch# set vlans vlan-id 20 l3-interface vlan20
admin@Switch# set l3-interface vlan-interface vlan10 address 192.168.1.10 prefix-length 24
admin@Switch# set l3-interface vlan-interface vlan20 address 192.168.2.1 prefix-length 24
```

Step2 Configure route reachability on the network.

```
admin@Switch# set protocols ospf router-id 1.1.1.1
admin@Switch# set protocols ospf area 0
admin@Switch# set protocols ospf network 192.168.1.0/24 area 0
admin@Switch# set protocols ospf network 192.168.2.0/24 area 0
admin@Switch# set ip routing enable true
```

Step3 Enable SNMP trap.

```
admin@Switch# set l3-interface loopback lo address 192.168.3.30 prefix-length 32
admin@Switch# set protocols snmp community Pica8-data-center
admin@Switch# set protocols snmp trap-group targets 192.168.3.1 security-name Pica8-data-center
admin@Switch# set protocols snmp trap-group source-interface loopback
```

Step4 Configure RMON ethernet statistics and history statistics.

```
admin@Switch# set protocols snmp rmon statistics 1 interface ge-1/1/2
admin@Switch# set protocols snmp rmon statistics 1 owner owner_pica8
```

```
admin@Switch# set protocols snmp rmon history 1 interface ge-1/1/2
admin@Switch# set protocols snmp rmon history 1 owner owner_pica8
```

Step5 Configure RMON event type to log and trap.

```
admin@Switch# set protocols snmp rmon event 1 type log-trap
admin@Switch# set protocols snmp rmon event 1 community Pica8-data-center
admin@Switch# set protocols snmp rmon event 1 description test
admin@Switch# set protocols snmp rmon event 1 owner public
```

Step6 Configure RMON alarm to monitor MIB variable 1.3.6.1.2.1.16.1.1.1.4.1, and the rising threshold to 600, falling threshold to 400.

```
admin@Switch# set protocols snmp rmon alarm 1 variable 1.3.6.1.2.1.16.1.1.1.4.1
admin@Switch# set protocols snmp rmon alarm 1 interval 20
admin@Switch# set protocols snmp rmon alarm 1 sample-type delta
admin@Switch# set protocols snmp rmon alarm 1 rising-threshold 600
admin@Switch# set protocols snmp rmon alarm 1 rising-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 falling-threshold 400
admin@Switch# set protocols snmp rmon alarm 1 falling-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 owner public
```

Step7 Commit after completing all the above configurations.

```
admin@Switch# commit
```

Verifying the Configuration

- The **run show rmon statistics** command can be used to view RMON Ethernet statistics information.

```
admin@Switch# run show rmon statistics
Entry 1 on ge-1/1/2 is active, and owned by owner_pica8,
    Monitors ifIndex.2 which has
    Received 354601 octets, 3643 packets,
    0 broadcast and 0 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    dropped packet events (due to lack of resources):0.
    packets received of length (in octets):
        64: 0, 65-127: 3524, 128-255: 119,
        256-511: 0, 512-1023: 0, 1024-1518: 0
```

- The **run show rmon history** command can be used to view RMON history statistics information.

```
admin@Switch# run show rmon history
Entry 1 on ge-1/1/2 is active, and owned by owner_pica8,
    Monitors ifIndex.2 every 10 seconds, bucket is 50,
        Sample # 1 began measuring at 0:43:22
            Received 576000 octets, 9000 packets,
            0 broadcast and 9000 multicast packets,
            0 undersized and 0 oversized packets,
            0 fragments and 0 jabbers,
            0 CRC alignment errors and 0 collisions.
            network utilization is estimated at 0
        Sample # 2 began measuring at 0:43:32
            Received 0 octets, 0 packets,
            0 broadcast and 0 multicast packets,
            0 undersized and 0 oversized packets,
            0 fragments and 0 jabbers,
            0 CRC alignment errors and 0 collisions.
            network utilization is estimated at 0
        Sample # 3 began measuring at 0:43:42
            Received 0 octets, 0 packets,
            0 broadcast and 0 multicast packets,
            0 undersized and 0 oversized packets,
            0 fragments and 0 jabbers,
            0 CRC alignment errors and 0 collisions.
```

```
            network utilization is estimated at 0
```

- The **run show rmon events** command can be used to view RMON event information.

```
admin@Switch# run show rmon events
Entry 1 is active, and owned by public,
    Description is test,
    Event firing causes trap to community Pica8-data-center,
    Last event fired at 0:01:19,
    Current uptime 1:02:17.
```

- The **run show rmon eventlog** command can be used to view RMON event log information.

```
admin@Switch# run show rmon eventlog
Entry 1 owned by public is VALID.
    Generates eventLog 1.1 at 2:01:19.
    Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarmEntry 1, equal or more than 600 with alarm value 3698
```

- The **run show rmon alarms** command can be used to view RMON alarms information.

```
admin@Switch# run show rmon alarms
Entry 1 is active, and owned by public
    Monitors 1.3.6.1.2.1.16.1.1.1.4.1 every 20 seconds
    Taking delta samples, last value was 369804
    Rising threshold is 600, assigned to event 1
    Falling threshold is 400, assigned to event 1
    On startup enable rising or falling alarm
```

RESTCONF Configuration

- Introduction of RESTCONF
- RESTCONF Operation Methods
- Configuring RESTCONF

Introduction of RESTCONF

- Overview
  - Figure 1. RESTCONF Components
- YANG Model
- Authentication
- HTTP Status Code
- RESTCONF Error Codes

NOTE:

When the `picos-web` service is enabled, it occupies ports 80 and 443 by default. Since `RESTCONF` also uses these default ports, it may fail to function properly, returning authentication errors. To use `RESTCONF` on switches with `picos-web` enabled, you must configure RESTCONF to use a custom port.

Overview

RESTCONF is a network configuration management protocol that uses HTTP methods, including OPTIONS, HEAD, GET, POST, PATCH, PUT and DELETE, to provide a set of Create, Read, Update, Delete (CRUD) operations on YANG-defined datastore to manage network devices.

RESTCONF is developed based on the integration of NETCONF and HTTP protocols, which can be implemented on a device that supports the NETCONF protocol.

RESTCONF provides a programming interface in line with the popular RESTful style, providing users with the ability to efficiently develop Web-based operation and maintenance tools.

RESTCONF Components

As shown in **Figure 1**, the RESTCONF protocol consists of two parts: RESTCONF Client and Server.

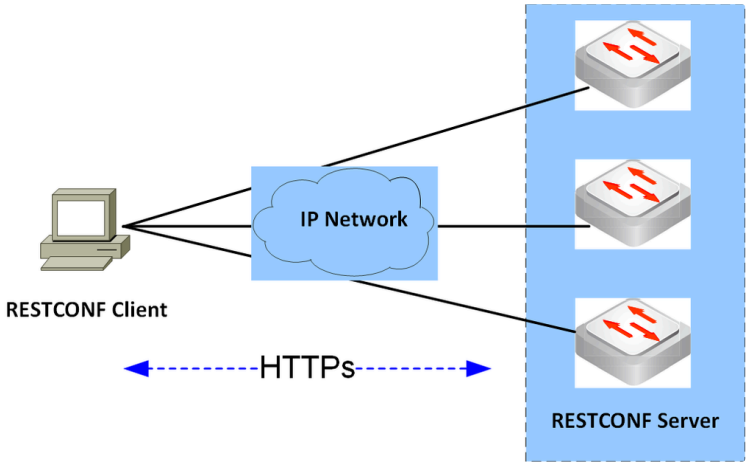
- RESTCONF Client

The client utilizes the RESTCONF protocol for system management of network devices. The client sends HTTP requests to the server to create, delete, modify or query one or more data, encoded in XML or JSON format.

- RESTCONF Server

The server device is used to maintain the information data of the managed devices. When receiving a HTTP request from the RESTCONF client, the server parses and processes the request message, and then returns a response to the client.

Figure 1. RESTCONF Components



The information that the client obtains from the running server includes configuration data and status data.

- The client can query the status data and the configuration data.
- The client can modify the configuration data and manipulate it to achieve the desired state of the server.
- The client cannot modify the status data, which mainly includes the running status and statistical information of the server.

Advantage

- RESTCONF provides RESTful style programming interface to support Web development.
- Adopting XML or JSON encoding.
- Standardized interface, compatible with devices from multiple manufacturers, can reduce development and maintenance costs.
- Good extensibility, different manufacturer devices can define their own protocol operation.

YANG Model

Same as NETCONF, RESTCONF also works based on YANG.

Most YANG files independent of the device type are placed in the following path:

/pica/etc/common/data-models.

```
root@PICOS:/pica/etc/common/data-models# ls -lt *.yang
-rw-r--r-- 1 root root 178165 May 19  2023 bgp.yang
-rw-r--r-- 1 root root   4487 May 12  2023 arp.yang
-rw-r--r-- 1 root root  56906 May  5  2023 ospfv2.yang
-rw-r--r-- 1 root root  22047 May  5  2023 ospfv3.yang
-rw-r--r-- 1 root root  16808 Apr 12  2023 bfd.yang
-rw-r--r-- 1 root root   7163 Apr 12  2023 cos-with-pfc.yang
-rw-r--r-- 1 root root   8350 Apr 12  2023 dhcp.yang
-rw-r--r-- 1 root root  23978 Apr 12  2023 firewall-no-icmp-type-code.yang
-rw-r--r-- 1 root root  24752 Apr 12  2023 firewall.yang
-rw-r--r-- 1 root root   2416 Apr 12  2023 igmp.yang
-rw-r--r-- 1 root root   8168 Apr 12  2023 igmpsnooping.yang
-rw-r--r-- 1 root root   4244 Apr 12  2023 lacp.yang
-rw-r--r-- 1 root root   5081 Apr 12  2023 mlag.yang
-rw-r--r-- 1 root root  26129 Apr 12  2023 mstp.yang
-rw-r--r-- 1 root root   5118 Apr 12  2023 ovsdb.yang
-rw-r--r-- 1 root root   7986 Apr 12  2023 pim.yang
-rw-r--r-- 1 root root  58523 Apr 12  2023 routing.yang
-rw-r--r-- 1 root root   5240 Apr 12  2023 sflow.yang
```

```
-rw-r--r-- 1 root root  10446 Apr 12  2023 snmp.yang
-rw-r--r-- 1 root root  13186 Apr 12  2023 static-routes.yang
-rw-r--r-- 1 root root  17509 Apr 12  2023 vlan-interface.yang
-rw-r--r-- 1 root root   8591 Apr 12  2023 vlans.yang
-rw-r--r-- 1 root root  11408 Apr 12  2023 vrrp.yang
-rw-r--r-- 1 root root   9920 Apr 12  2023 vxlans.yang
-rw-r--r-- 1 root root   5173 Aug 24  2022 dot1x.yang
-rw-r--r-- 1 root root   6062 Aug 12  2022 cos-without-pfc.yang
-rw-r--r-- 1 root root  16760 Aug 12  2022 ietf-inet-types.yang
-rw-r--r-- 1 root root  18034 Aug 12  2022 ietf-yang-types.yang
-rw-r--r-- 1 root root   5475 Aug 12  2022 ipfix.yang
-rw-r--r-- 1 root root   6944 Aug 12  2022 lldp.yang
-rw-r--r-- 1 root root   1411 Aug 12  2022 mfea.yang
-rw-r--r-- 1 root root   1629 Aug 12  2022 mpls.yang
-rw-r--r-- 1 root root   4825 Aug 12  2022 neighbour.yang
-rw-r--r-- 1 root root   8833 Aug 12  2022 policy.yang
-rw-r--r-- 1 root root   4592 Aug 12  2022 rip.yang
-rw-r--r-- 1 root root   3669 Aug 12  2022 ripng.yang
-rw-r--r-- 1 root root  50887 Aug 12  2022 system.yang
-rw-r--r-- 1 root root   4126 Aug 12  2022 udld.yang
-rw-r--r-- 1 root root    871 Aug 12  2022 version.yang
-rw-r--r-- 1 root root   4515 Aug 12  2022 xovs.yang
```

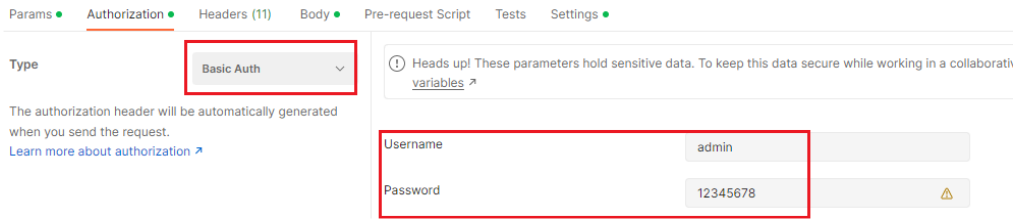
The yang files related to the device type are placed in the following path. This path contains a soft link to the yang file above, use an ellipsis instead.

```
root@PICOS:/pica/etc/as5712_54x/data-models# ls -lt *.yang
……
-rw-r--r-- 1 root root 58741 Apr 12  2023 interface.yang
-rw-r--r-- 1 root root  2211 Aug 12  2022 stm.yang
```

Authentication

RESTCONF supports setting authorization to “Basic Auth”, the username and password should be set to the same as the accounts used for authentication of the RESTCONF server.

In the HTTPs request message sent by the client, you need to fill in the authentication information correctly to ensure that the connection between the RESTCONF client and server can be established successfully.



HTTP Status Code

RESTCONF uses the Status-Line part of an HTTP response message to inform clients of their request’s result. HTTP defines these standard status codes that can be used to convey the results of a client’s request.

Table 1. HTTP status codes

Status Code	Description
200 OK	Indicates that the request has succeeded.

201 Created	Indicates that the request has succeeded and a new resource has been created as a result.
204 No Content	The server has fulfilled the request but does not need to return a response body. The server may return the updated meta information.
400 Bad Request	The request could not be understood by the server due to incorrect syntax. The client SHOULD NOT repeat the request without modifications.
401 Unauthorized	Indicates that the request requires user authentication information. The client MAY repeat the request with a suitable Authorization header field
403 Forbidden	Unauthorized request. The client does not have access rights to the content. Unlike 401, the client's identity is known to the server.
404 Not Found	The server cannot find the requested resource.
405 Method Not Allowed	The request HTTP method is known by the server but has been disabled and cannot be used for that resource.
408 Request Timeout	Indicates that the server did not receive a complete request from the client within the server's allotted timeout period.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server.
412 Precondition Failed	The client has indicated preconditions in its headers which the server does not meet.
413 Request Entity Too Large	Request entity is larger than limits defined by server.
414 Request-URI Too Long	The URI requested by the client is longer than the server can interpret.
415 Unsupported Media Type	The media-type in Content-type of the request is not supported by the server.
500 Internal Server Error	The server encountered an unexpected condition that prevented it from fulfilling the request.
501 Not Implemented	The HTTP method is not supported by the server and cannot be handled.

RESTCONF Error Codes

The tree of YANG model <errors> is defined as follows:

```
+---- errors
      +---- error*
         +---- error-type       enumeration
         +---- error-tag        string
         +---- error-app-tag?   string
         +---- error-path?      instance-identifier
         +---- error-message?   string
         +---- error-info?
```

When an error occurs, the server returns a response message carried with above error information.

- **error-type**

The value of error-type can be：

Value	Description
transport	Transport Layer
tpc	RPC Layer
protocol	Operation Layer
application	Application Layer

- **error-tag**

<error-tag>	Error description	Status code
in-use	The requested resource is already in use	409
invalid-value	The parameter value in the request is incorrect	400, 404 or 406
too-big	Request or reply messages are too large to process	413 or 400
missing-attribute	Missing attribute on element node	400
bad-attribute	Attribute error on element node	400
unknown-attribute	Unknown attribute on element node	400
bad-element	The element node value is incorrect	400
unknown-element	Unrecognized elements	400
unknown-namespace	Unrecognized namespaces	400
access-denied	Access denied	401 or 403
lock-denied	The configuration process is locked	409
resource-denied	Insufficient resources to complete the request	409
rollback-failed	Rollback failure	500
data-exists	The data already exists and POST creates a duplicate record	409
data-missing	Deleting a non-existent object returns this error	409
operation-not-supported	The operation is not supported. For example, POST and DELETE	405 or 501

	operations are not supported for current container nodes	
operation-failed	Operation execution failed	412 or 500
partial-operation	Some operations failed	500
malformed-message	The message format is incorrect	400

- **error-app-tag:** Indicates a specific error type.
- **error-path:** Represents the location where the error occurred.
- **error-message:** Indicates detailed error information.
- **error-info:** Indicates the description of error parameters.

For example,

- Example 1: Input an error path when using GET method causes error: **"error-type": "application"**.



The response result is:

```
400 Bad Request
{
    "ietf-restconf:errors": {
        "error": {
            "error-type": "application",
            "error-tag": "unknown-element",
            "error-info": {
                "bad-element": "vlan"
            },
            "error-severity": "error",
            "error-message": "No such yang module prefix"
        }
    }
}
```

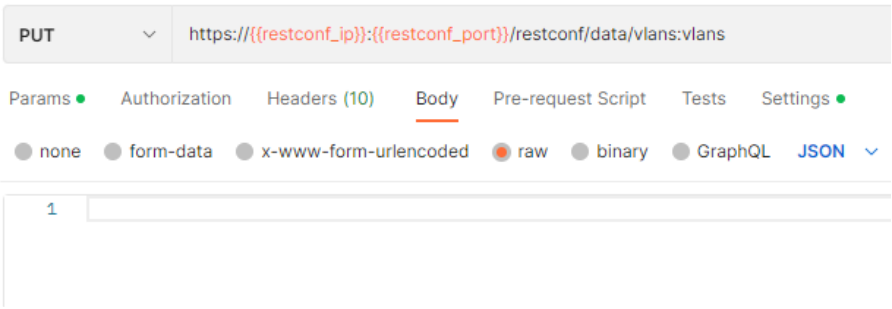
- Example 2: Input a non-exist path when using PATCH method causes error: **"error-type": "protocol"**.



The response result is:

```
400 Bad Request
{
    "ietf-restconf:errors": {
        "error": {
            "error-type": "protocol",
            "error-tag": "invalid-value",
            "error-severity": "error",
            "error-message": "API-resource type"
        }
    }
}
```

- Example 3: No data was provided when using PUT method causes error: **"error-type": "rpc"**.



The response result is:

```
400 Bad Request
{
    "ietf-restconf:errors": {
        "error": {
            "error-type": "rpc",
            "error-tag": "malformed-message",
            "error-severity": "error",
            "error-message": "The message-body MUST contain exactly one instance of the expected data resource"
        }
    }
}
```

RESTCONF Operation Methods

- OPTIONS
- HEAD
- GET
- POST
- PATCH
- PUT
- DELETE

RESTCONF supports **OPTIONS, HEAD, GET, POST, PATCH, PUT** and **DELETE** methods which can be used to query and modify resources. If RESTCONF request sent from the client contains data to be operated on a specific method, the data will be placed in either XML or JSON format in the Body.

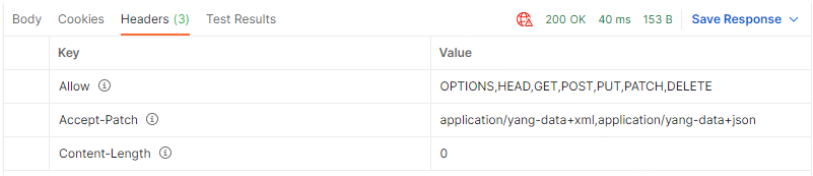
The following sections describe the usage of each method with specific examples, where HTTP client tools Postman and PyCharm are used.

OPTIONS

- Function description: The client sends the OPTIONS method to discover which methods the server supports for a particular resource (for example, GET, POST, DELETE).
- URL: https://device_ip:port/restconf/data
- Example: Request from RESTCONF client using Postman



The response result is:



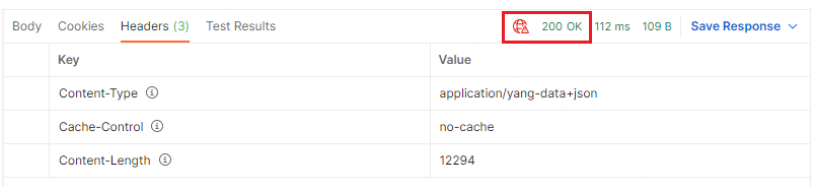
In the result,

- "**Allow**" shows the RESTCONF methods supported by the server. In this example, the RESTCONF methods supported by the server are OPTIONS, HEAD, GET, POST, PATCH, PUT and DELETE.
- "**Accept-Patch**" shows the data formats supported by the PATCH method. In this example, the data formats can be accepted are **application/yang-data+xml** and **application/yang-data+json**.

HEAD

- Function description: The HEAD method is sent by the client to query whether the configuration data and status data exist, only the Header fields that would be returned for the comparable GET method, without the response message-body. It is supported for all resources that support the GET method.
- URL: https://device_ip:port/restconf/data/modulename:node
- Example: Request from RESTCONF client using Postman

The response result is:

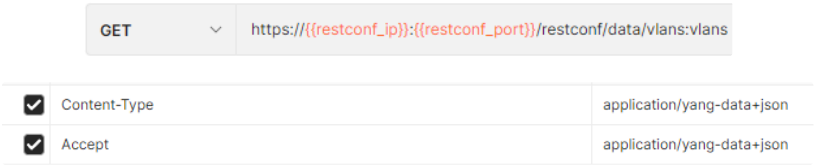


If the query data exists, the "**200 OK**" status code is returned, you can use GET method to get the data information.

GET

- Function description: The GET method is sent by the client to retrieve data and metadata for a resource.

- URL: https://device_ip:port/restconf/data/modulename:node
- Example 1: Request from RESTCONF client using Postman



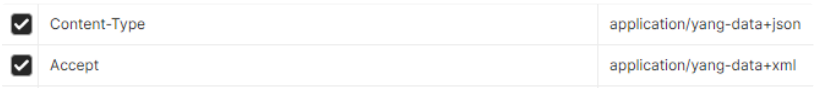
As shown in above figure,

- "**Content-Type**" field in the header defines the body format of request messages.
- "**Accept**" field defines the body format of response messages.

If set "Accept" field to "application/yang-data+json", the response result received is in JSON format:



If set "Accept" field to "application/yang-data+xml":



The response result received is in XML format:



- Example 2: Request from RESTCONF client using PyCharm

```
import requests
from requests.auth import HTTPBasicAuth
import json
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

AUTH = HTTPBasicAuth('admin', '12345678')
ACCEPT_TYPE  = 'application/yang-data+json'
CONTENT_TYPE = 'application/yang-data+json'
HEADERS = { 'Accept': ACCEPT_TYPE, 'Content-Type': CONTENT_TYPE }

def get_request(url):
    response = requests.get(url, auth=AUTH, headers=HEADERS, verify=False)
    print("URL:", url)
    print("ret code:", response.status_code)
    if response.status_code in [200]:
        print("Successful")
    else:
        print("Error in API Request")
    output = json.loads(response.text)
    print(output)
```

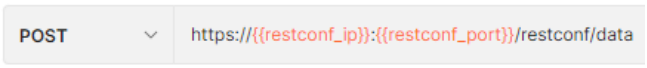
```
22
23 url = "https://10.10.51.186/restconf/data/vlans:vlans"
24
25 get_request(url)
```

The response result is:

```
1 URL: https://10.10.51.186/restconf/data/vlans:vlans
2 ret code: 200
3 Successful
4 {'vlans:vlans': {'vlan-id': [{'id': '1000', 'vlan-name': 'test1000'}]}}
```

POST

- Function description: The POST method is sent by the client to create top-level resource or sub-resource.
- URL: https://device_ip:port/restconf/data
- Example 1: Request from RESTCONF client using Postman



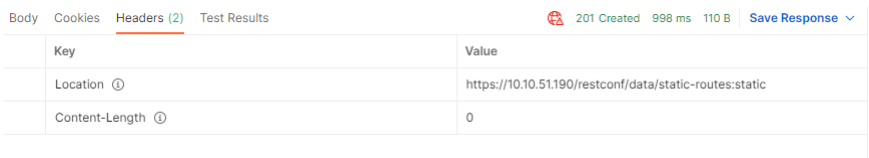
Data format defined in the header:



The expected settings are written to the body in JSON format:



Response is:



The result can be shown on the managed network device:

```
1 admin@PICOS# The configuration has been changed by user root
2 DELTAS:
3     protocols {
4         static {
5             route 8.8.8.0/24 {
6                 next-hop 10.10.10.10
7             }
8         }
9     }
10 admin@PICOS# show protocols static
11     route 8.8.8.0/24 {
```

```
        next-hop 10.10.10.10
    }
```

- Example 2: we can write the body in XML format in PyCharm:

```
import requests
from requests.auth import HTTPBasicAuth
import json
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

AUTH = HTTPBasicAuth('admin', '12345678')
ACCEPT_TYPE  = 'application/yang-data+json'
CONTENT_TYPE = 'application/yang-data+xml'
HEADERS = { 'Accept': ACCEPT_TYPE, 'Content-Type': CONTENT_TYPE }

def get_request(url):
    payload = '<static xmlns="http://pica8.com/xorplus/static-routes" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">' \
              '<route>' \
                '<name>8.8.8.0/24</name>' \
                '<next-hop>' \
                  '<ip-address>10.10.10.10</ip-address>' \
                '</next-hop>' \
              '</route>' \
              '</static>'
    response = requests.post(url, auth=AUTH, headers=HEADERS, verify=False,data=payload)
    print("URL: ", url)
    print(response.status_code)
    if response.status_code in [201]:
        print("Successful")
    else:
        print("Error in API Request")
    #output = json.loads(response.text)
    print(response.text)

url = "https://10.10.51.186/restconf/data"

get_request(url)
```

The response result is:

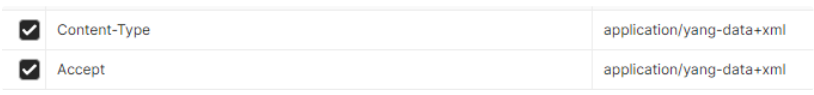
```
URL:  https://10.10.51.186/restconf/data
201
Successful
```

PATCH

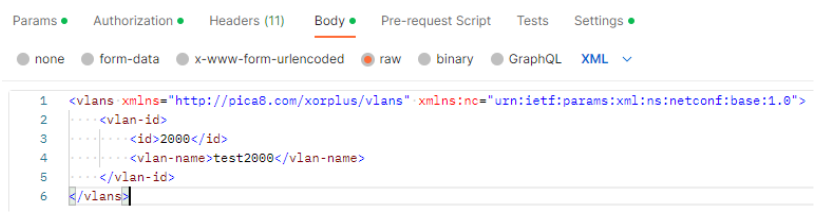
- Function description: The PATCH method is sent by the client to modify the configuration data.
- URL: https://device_ip:port/restconf/data/modulename:node
- Example 1: Request from RESTCONF client using Postman



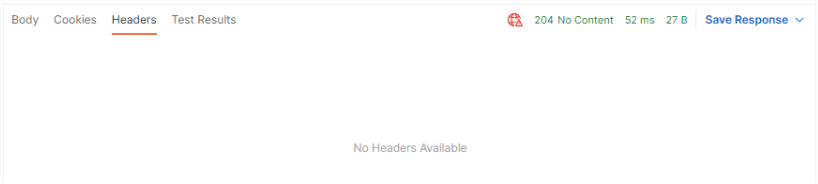
Data format defined in the header:



The expected settings are written to the body in XML format:



Response received is:



Then the configuration has been set to the device.

```
admin@PICOS# show vlans
    vlan-id 1000 {
        vlan-name: "test1000"
    }

admin@PICOS# The configuration has been changed by user root
DELTAS:
    vlans {
        vlan-id 2000 {
            vlan-name: "test2000"
        }
    }
admin@PICOS#
admin@PICOS# show vlans
    vlan-id 1000 {
        vlan-name: "test1000"
    }
    vlan-id 2000 {
        vlan-name: "test2000"
    }
```

- Example 2: we can write the body section in JSON format in PyCharm

```
import requests
from requests.auth import HTTPBasicAuth
import json
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

AUTH = HTTPBasicAuth('admin', '12345678')
ACCEPT_TYPE  = 'application/yang-data+json'
CONTENT_TYPE = 'application/yang-data+json'
HEADERS = { 'Accept': ACCEPT_TYPE, 'Content-Type': CONTENT_TYPE }

def get_request(url):
    payload = '{"vlans:vlans":{"vlan-id":[{"id":"2000","vlan-name":"test2000"}]}}'
    response = requests.patch(url, auth=AUTH, headers=HEADERS, verify=False, data=payload)
    print("URL:", url)
    print("ret code:", response.status_code)
    if response.status_code in [204]:
        print("Successful")
    else:
        print("Error in API Request")
    #output = json.loads(response.text)
    print(response.text)

url = "https://10.10.51.186/restconf/data/vlans:vlans"

get_request(url)
```

The response result is:

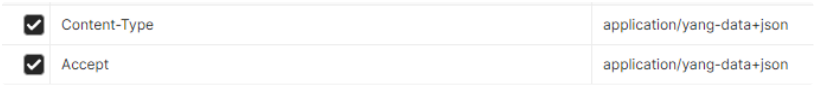
```
URL: https://10.10.51.186/restconf/data/vlans:vlans
ret code: 204
Successful
```

PUT

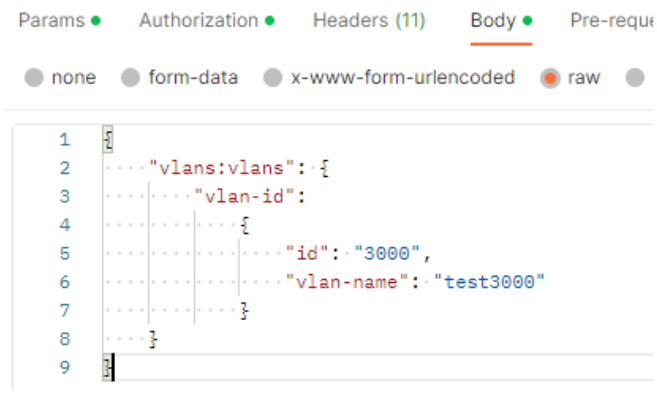
- Function description: The PUT method is sending the latest configuration to the device to replace the data on the device.
- URL: https://device_ip:port/restconf/data/modulename:node
- Example 1: Request from RESTCONF client using Postman



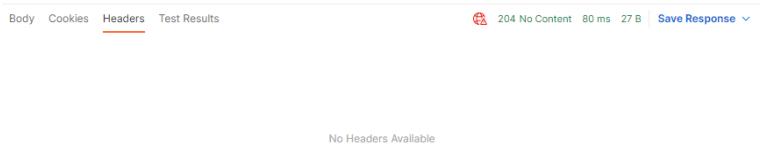
Data format defined in the header:



The expected settings are written to the body in JSON format:



Response is:



The expected configuration takes effect and the old configuration is deleted.

```
admin@PICOS# show vlans
    vlan-id 1000 {
        vlan-name: "test1000"
    }
    vlan-id 2000 {
        vlan-name: "test2000"
}
admin@PICOS# The configuration has been changed by user root
DELETIONS:
    vlans {
        vlan-id 1000
        vlan-id 2000
    }
DELTAS:
    vlans {
        vlan-id 3000 {
            vlan-name: "test3000"
        }
    }
admin@PICOS# show vlans
    vlan-id 3000 {
        vlan-name: "test3000"
    }
```

- Example 2: we can do it in PyCharm:

```
import requests
from requests.auth import HTTPBasicAuth
import json
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

AUTH = HTTPBasicAuth('admin', '12345678')
ACCEPT_TYPE  = 'application/yang-data+json'
```

```
CONTENT_TYPE = 'application/yang-data+json'
HEADERS = { 'Accept': ACCEPT_TYPE, 'Content-Type': CONTENT_TYPE }

def get_request(url):
    payload = '{"vlans:vlans":{"vlan-id":{"id":"3000","vlan-name":"test3000"}}}'
    response = requests.put(url, auth=AUTH, headers=HEADERS, verify=False, data=payload)
    print("URL:", url)
    print("ret code:", response.status_code)
    if response.status_code in [204]:
        print("Successful")
    else:
        print("Error in API Request")
    #output = json.loads(response.text)
    print(response.text)

url = "https://10.10.51.186/restconf/data/vlans:vlans"

get_request(url)
```

The response result is:

```
URL: https://10.10.51.186/restconf/data/vlans:vlans
ret code: 204
Successful
```

DELETE

- Function description: The DELETE method is used to delete the node or data specified by the URL.

There are several application scenarios are supported when using DELETE method:

Scenario 1: Delete all the configurations of a specified module

- URL: https://device_ip:port/restconf/data/modulename:node
- Example: Request from RESTCONF client using Postman



On the managed network device, we can see that the configurations under module "**static-route**" is removed:

```
admin@PICOS# show protocols static
    route 8.8.8.0/24 {
        next-hop 10.10.10.10
    }

admin@PICOS# The configuration has been changed by user root
DELETIONS:
    protocols {
        static {
        }
    }
admin@PICOS# show protocols static
ERROR: try to show a non existing configure tree node.
```

Scenario 2: Delete specified list member

- URL: https://device_ip:port/restconf/data/modulename:node/container
- Example: Request from RESTCONF client using Postman



On the managed network device, we can see that *vlan-id=1000* in the vlan-id list is removed:

```
admin@PICOS# show vlans
    vlan-id 1000 {
        vlan-name: "test1000"
    }
    vlan-id 2000 {
        vlan-name: "test2000"
    }

```

```
admin@PICOS# The configuration has been changed by user root
DELETIONS:
    vlans {
        vlan-id 1000
    }
admin@PICOS# show vlans
    vlan-id 2000 {
        vlan-name: "test2000"
    }
```

Scenario 3: Delete specified container

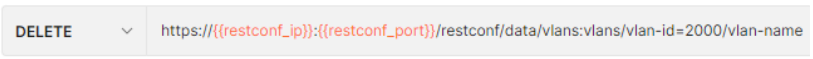
- URL: https://device_ip:port/restconf/data/modulename:node[/parant-container]/child-container
- Example: Request from RESTCONF client using Postman

On the managed network device, we can see that child container family in specified parent container interface is removed:

```
admin@PICOS# show interface gigabit-ethernet xe-1/1/6
    mtu: 2000
    family {
        ethernet-switching {
        }
    }
admin@PICOS# The configuration has been changed by user root
DELETIONS:
    interface {
        gigabit-ethernet "xe-1/1/6" {
            family {
            }
        }
    }
admin@PICOS# show interface gigabit-ethernet xe-1/1/6
    mtu: 2000
```

Scenario 4: Delete specified leaf

- URL: https://device_ip:port/restconf/data/modulename:node/container/leaf
- Example: Request from RESTCONF client using Postman

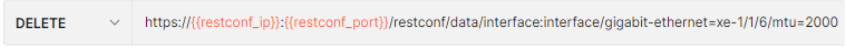


On the managed network device, we can see that leaf "**vlan-name**" is removed:

```
admin@PICOS# show vlans
    vlan-id 2000 {
        vlan-name: "test2000"
    }

admin@PICOS# The configuration has been changed by user root
DELETIONS:
    vlans {
        vlan-id 2000 {
            vlan-name: "test2000"
        }
    }
admin@PICOS# show vlans
    vlan-id 2000 {
    }
```

Scenario 5: Restores a leaf that has a default value to its default value

- URL: https://device_ip:port/restconf/data/modulename:node/container/leaf=configured_value
- Example: Request from RESTCONF client using Postman



On the managed network device, we can see that the MTU configuration is removed and restored to the default value 1514:

```
admin@PICOS# show interface gigabit-ethernet xe-1/1/6
```

```
    mtu: 2000

admin@PICOS# The configuration has been changed by user root
DELETIONS:
    interface {
        gigabit-ethernet "xe-1/1/6" {
            mtu: 2000
        }
    }
admin@PICOS# show interface gigabit-ethernet xe-1/1/6

```

Configuring RESTCONF

- Configuration on RESTCONF Server
- Configuration Example
  - Networking Requirements
    - Figure 1. Application Scenarios for RESTCONF
  - Procedure

NOTE:

When the `picos-web` service is enabled, it occupies ports 80 and 443 by default. Since `RESTCONF` also uses these default ports, it may fail to function properly, returning authentication errors. To use `RESTCONF` on switches with `picos-web` enabled, you must configure RESTCONF to use a custom port.

Configuration on RESTCONF Server

Step 1 Enable RESTCONF on the server side.

set protocols restconf

Step 2 (Optional) Configure RESTCONF service listening port on the server side.

set protocols restconf port *<port-number>*

By default, the RESTCONF service port number is 443.

> **NOTE**:
>
> The RESTCONF service listening port in the HTTP request URL sent by RESTCONF Client needs to be consistent with the port configured on the server side.

Step 3 Commit the configurations.

commit

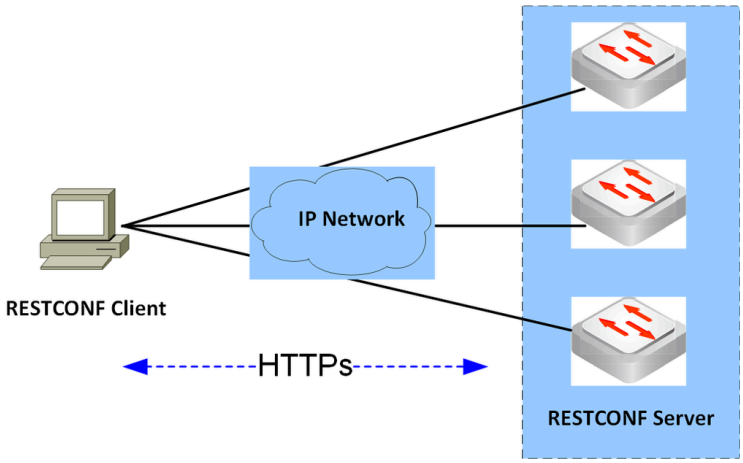
Configuration Example

Networking Requirements

When users want to manage network devices through a unified management device with high security and scalability, administrators can utilize RESTCONF protocol to remotely configure and manage network devices using HTTP methods, and monitor these devices in real-time.

As shown in **Figure 1**, RESTCONF Client and RESTCONF Server are connected to each other via an IP network. As an HTTPs client, RESTCONF Client sends HTTP requests to the RESTCONF Server, which is an HTTPs server, using the OPTIONS, HEAD, GET, POST, PATCH, PUT and DELETE methods to create, delete, modify or query one or more data, thus realizing the management of profiles through RESTCONF.

Figure 1. Application Scenarios for RESTCONF



Deploy and configure RESTCONF through the following approach:

1. Configure the RESTCONF Client and Server to achieve Layer 3 route reachability between them. This will not be detailed in the following configuration procedure.

2. Enable RESTCONF function and configure RESTCONF service listening port on the RESTCONF Server.

3. After completing the above configuration, the RESTCONF Client can send HTTP requests to the RESTCONF Server to remotely manage the network devices.

Procedure

Step 1 Enable RESTCONF on the server side.

```
admin@RESTCONF-Server# set protocols restconf
```

Step 2 (Optional) Configure RESTCONF service listening port on the server side.

```
admin@RESTCONF-Server# set protocols restconf port 1024
```

By default, the RESTCONF service listening port number is 443.

> **NOTE**:
>
> The RESTCONF service listening port in the HTTP request URL sent by RESTCONF Client needs to be consistent with the port configured on the server side.

Step 3 Commit the configurations.

```
admin@RESTCONF-Server# commit
```

EFM OAM Configuration

- Introduction of EFM OAM
- Configuring EFM OAM

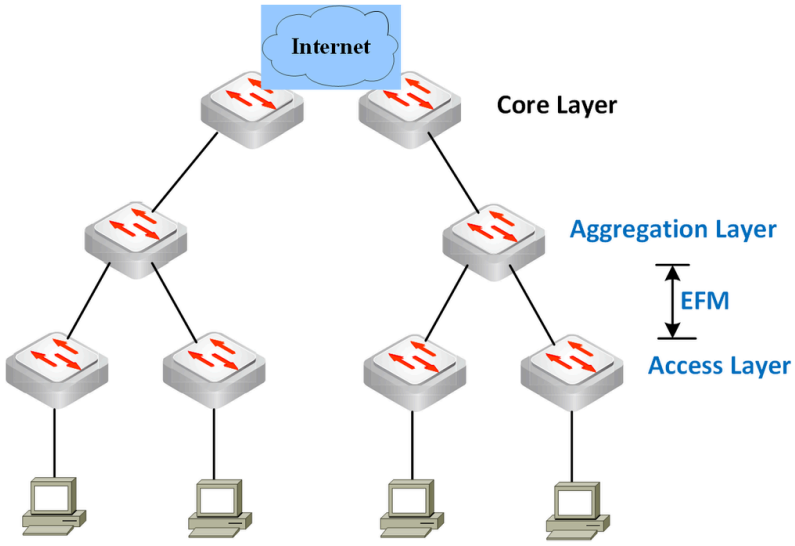
Introduction of EFM OAM

- Overview
- Types of EFM OAMPDU
- EFM OAM Mode
- EFM OAM Operation Mechanism
  - EFM OAM Discovery
  - Remote Loopback

Overview

Ethernet in the First Mile (EFM) is the Ethernet physical layer specification which is mainly used between the link of the access layer and the aggregation layer for Ethernet management and maintenance. EFM is the link-level OAM (Operation and Management). For the link between two directly connected devices, it provides link connectivity detection function, link failure monitoring function and remote loopback function.

Figure 1. Networking diagram for Ethernet OAM



Types of EFM OAMPDU

EFM works at the data link layer, and its protocol messages are called OAMPDUs (OAM Protocol Data Units). EFM detects and reports link status through periodic OAMPDUs between devices, enabling network administrators to manage the network effectively. **Table 1** shows the OAMPDUs types supported by PICOS.

Table 1. Types of EFM OAMPDU Supported by PICOS

OAMPDU Type	Description
Information OAMPDU	For EFM peer discovery, the OAM entity in the handshake phase periodically sends Information OAMPDUs at certain period to detect the connectivity of a link.

Loopback Control OAMPDU	It is used for remote loopback operation to control the OAM loopback state of the remote device, and to enable or disable the remote loopback function according to the remote loopback enabling or disabling information in the OAMPDU.

EFM OAM Mode

There are two EFM OAM modes: active mode and passive mode. EFM connections can only be initiated by active mode OAM entities, while passive mode OAM entities can only wait for connection requests from peer OAM entities. Different connection modes have different processing capabilities for OAMPDU which is shown in **Table 2**.

Table 2. Comparison of OAMPDU processing capability between active and passive modes

Processing capability of OAMPDU	Active Mode	Passive Mode
Initialization of Discovery process (initiating a connection request, i.e., sending an Information OAMPDU for the first handshake)	Support	Not Support
Responding to the Discovery initialization process (responding to connection requests)	Support	Support
Sending Information OAMPDU	Support	Support
Sending Loopback Control OAMPDU	Support	Not Support
Responding Loopback Control OAMPDU	Support (Requires active mode on the peer)	Support

EFM OAM Operation Mechanism

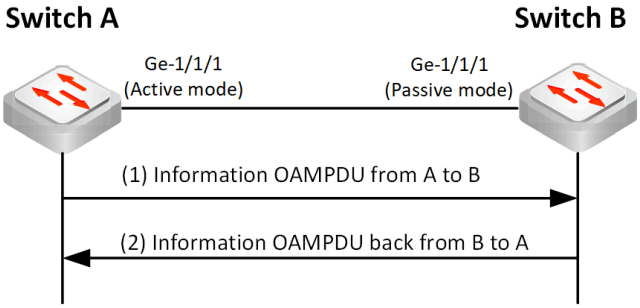
EFM OAM operation supported by PICOS includes Discovery and Remote Loopback.

EFM OAM Discovery

The implementation of EFM OAM function is based on EFM OAM connectivity. The process of establishing EFM OAM connectivity is also known as the Discovery phase, i.e., the process by which the local OAM entity discovers the remote OAM entity and establishes a stable connectivity with it.

When the EFM OAM function is enabled on an interface, and the EFM mode of the interface is active mode, then an EFM OAM connection is initiated from the interface to the remote end. During the process of establishing an EFM OAM connection, the connected OAM entities exchange the EFM OAM configuration information through the Information OAMPDUs to decide whether to establish an EFM OAM connection.

Figure 2. EFM OAM Discovery Diagram



As shown in **Figure 2**, interface Ge-1/1/1 on Switch A operates in EFM OAM active mode:

(1) Switch A sends an Information OAMPDU message to Switch B, which contains the EFM OAM configuration information of Switch A.

(2) After receiving the OAMPDU, Switch B compares the EFM OAM configuration of its own with Switch A, then replies to Switch A with an Information OAMPDU, which includes not only the EFM OAM configuration information for both Switch A and Switch B, but also the flag information indicating whether EFM OAM configurations of Switch B match Switch A.

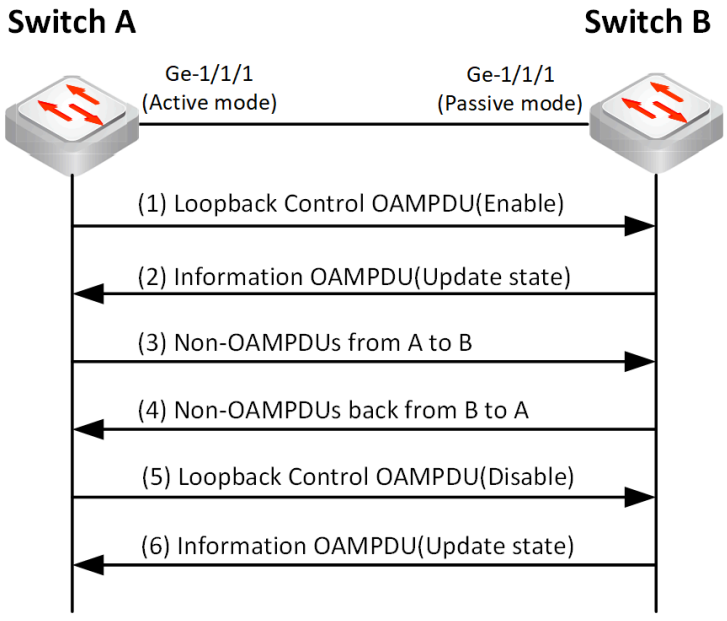
After receiving the response OAMPDU from Switch B, Switch A will then determine whether the EFM OAM configuration of Switch B matches its own configuration.

Through the above process, if the EFM OAM configurations of both sides match, the EFM OAM connection is established, after which the OAM entities at both ends will send Information OAMPDUs periodically to detect whether the connection is normal.

Remote Loopback

The remote loopback function means that when an OAM entity in active mode sends a message to the far end, the far end does not forward the message (except for OAMPDUs) based on its destination address after receiving it, but returns the message to the sender along the original path. It can be used to locate link faults and detect link quality: the network administrator can judge the link performance (including packet loss rate, delay, jitter, etc.) by observing the return of non-OAMPDU messages.

Figure 3. Schematic diagram of remote loopback



As shown in **Figure 3**, the EFM OAM connection between Switch A and Switch B is established, the interface Ge-1/1/1 of Switch A is working in EFM OAM active mode.

(1) When implementing the operations of start EFM OAM remote loopback tests on Switch A, Switch A sends a Loopback Control OAMPDU carried with remote loopback enabling information to Switch B, then waits for a reply.

(2) After receiving the OAMPDU, Switch B enters to the loopback state and replies to Switch A with an Information OAMPDU of the state change.

(3) & (4) In loopback state, Switch B returns all non-OAMPDU messages received along the original path to Switch A.

(5) When implementing the operations of stop EFM OAM remote loopback tests on Switch A, Switch A sends a Loopback Control OAMPDU carried with remote loopback disabling information to Switch B.

(6) When Switch B receives this OAMPDU, it exits the loopback state and replies to Switch A with an Information OAMPDU of the state change.

When remote loopback function is implemented, the interface no longer participates in any other Layer 2 or Layer 3 protocols. For example, Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). This is because when two connected ports are in a loopback session, no packets other than the OAM PDUs are sent to the CPU for software processing, services will be disrupted.

Configuring EFM OAM

- Configuration Notes and Constraints
- Configuring EFM OAM
- Example for Configuring EFM OAM
  - Networking Requirements
  - Procedure

Configuration Notes and Constraints

When configuring EFM OAM, pay attention to the following notes:

- An EFM connection cannot be established between two EFM OAM entities that are both in passive mode.
- Only the **active** mode end can run commands **ethernet-oam remote-loopback start interface** <*interface-name*> or **ethernet-oam remote-loopback stop interface** <*interface-name*> to start | stop EFM OAM remote loopback tests.
- Before starting the EFM OAM remote loopback tests, make sure:
  - The EFM OAM connection has been established successfully.
  - Users have to configure command **set protocols ethernet-oam interface** <*interface-name*> **remote-loopback supported** on the responding end to enable reactions to loopback control OAMPDUs from peers.
- Remote loopback cannot be configured on the same port as the loopback of the physical port.

Configuring EFM OAM

Step 1 Enable EFM OAM function on both end of the link.

set protocols ethernet-oam interface <*interface-name*> **enable** <**true | false**>

Step 2 Configure the EFM mode for this Ethernet port. By default, the EFM OAM interface works in **active** mode.

set protocols ethernet-oam interface <*interface-name*> **mode** <**active | passive**>

Step 3 Enable reactions to loopback control OAMPDUs from peers.

set protocols ethernet-oam interface <*interface-name*> **remote-loopback supported**

Step 4 (Optional) Configure EFM OAM timeout values.

set protocols ethernet-oam interface <*interface-name*> **remote-loopback timeout** <*loopback-timeout*>

set protocols ethernet-oam interface <*interface-name*> **timeout** <*oam-timeout*>

Step 5 Enable EFM OAM remote loopback tests on the specified port.

NOTEs:

- The commands **ethernet-oam remote-loopback start interface** and **ethernet-oam remote-loopback stop interface** are operational mode commands which should be executed under the prompt “admin@PICOS>”.
- Only the **active** mode end can run commands **ethernet-oam remote-loopback start interface** <*interface-name*> or **ethernet-oam remote-loopback stop interface** <*interface-name*> to start| stop EFM OAM remote loopback tests.
- Before starting the EFM OAM remote loopback tests, make sure:
  - The EFM OAM connection has been established successfully.

- Users have to configure command **set protocols ethernet-oam interface** *<interface-name>* **remote-loopback supported** on the responding end to enable reactions to loopback control OAMPDUs from peers.

- It is not allowed to modify EFM OAM mode when remote loopback function is implemented.

ethernet-oam remote-loopback start interface *<interface-name>*

Step 6 Stop EFM OAM remote loopback tests on the specified port.

ethernet-oam remote-loopback stop interface *<interface-name>*

Step 7 Commit the configuration.

commit

Step 8 View EFM OAM configuration information, session status and interface statistics.

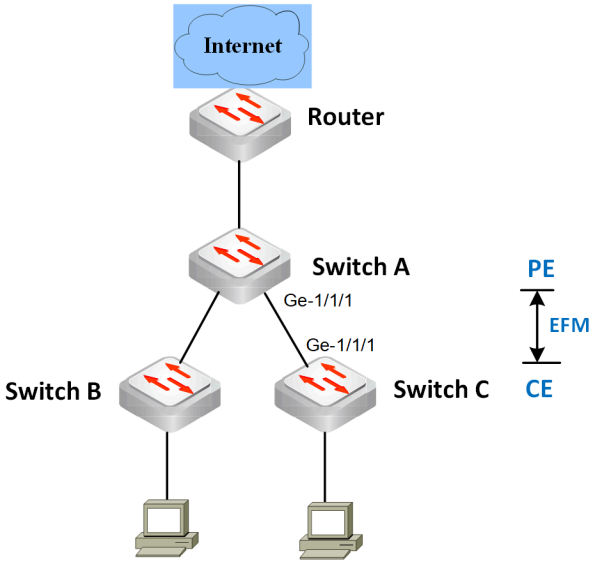
run show ethernet-oam [**interface** *<interface-name>*]

run show ethernet-oam statistics [**interface** *<interface-name>*]

Example for Configuring EFM OAM

Networking Requirements

Figure 1. EFM OAM Configuration Example



As shown in **Figure 1**, the link between Switch C to Switch A is a newly deployed network. The administrator hopes to achieve the following network management:

- Test network connectivity and quality before enabling the new network.
- Dynamically monitor the link quality after the link is properly enabled.

Follow the configuration roadmap below to configure EFM function:

1. Configure EFM basic functions on Switch A and Switch C devices to achieve automatic detection of link connectivity.
2. Configure EFM remote loopback on Switch A and Switch C to conduct link connectivity and performance testing.

Procedure

Step 1 Configure EFM basic function.

a) Enable EFM OAM function on interface ge-1/1/1 on Switch A.

```
admin@SwitchA# set protocols ethernet-oam interface ge-1/1/1 enable true
```

b) Configure the EFM OAM mode for this Ethernet port.

```
admin@SwitchA# set protocols ethernet-oam interface ge-1/1/1 mode active
admin@SwitchA# commit
```

c) Enable EFM OAM function on interface ge-1/1/1 on Switch C.

```
admin@SwitchC# set protocols ethernet-oam interface ge-1/1/1 enable true
```

d) Configure the mode of EFM OAM mode for this Ethernet port.

```
admin@SwitchC# set protocols ethernet-oam interface ge-1/1/1 mode passive
admin@SwitchC# commit
```

e) Verify the Configuration.

If the EFM configurations of Switch A and Switch C are correct, a connection will be established between them after successful negotiation in the Discovery phase. Run the command **run show ethernet-oam** on Switch A or Switch C, you can see that the EFM OAM protocol status of interface ge-1/1/1 is **SEND_ANY**.

```
admin@SwitchC# run show ethernet-oam
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          passive
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   no loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:5c:8c:21
    OUI:               48:6e:73
    PDU revision:      3
    OAM Mode:          active
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
```

Step 2 Enable remote loopback.

a) Enable reactions to loopback control OAMPDUs from peers on Switch C.

```
admin@SwitchC# set protocols ethernet-oam interface ge-1/1/1 remote-loopback supported
admin@SwitchC# commit
```

b) Start EFM OAM remote loopback tests on interface ge-1/1/1 on Switch A.

> **NOTE**s:

- The commands **ethernet-oam remote-loopback start interface** and **ethernet-oam remote-loopback stop interface** are operational mode commands which should be executed under the prompt “admin@PICOS>”.
- Before starting the EFM OAM remote loopback tests:
  - The EFM OAM connection has been established successfully.
  - Users have to configure command **set protocols ethernet-oam interface** <*interface-name*> **remote-loopback supported** on the responding end to enable reactions to loopback control OAMPDUs from peers.

```
admin@SwitchA> ethernet-oam remote-loopback start interface ge-1/1/1
```

c) Verify the Configuration.

- After successfully configuring EFM remote loopback, run the command **run show ethernet-oam**, and you can see that the loopback status is **local loopback** on Switch C and **remote loopback** on Switch A.

```
admin@SwitchC# run show ethernet-oam
--------------------------------------------------
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          passive
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   local loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:5c:8c:21
    OUI:               48:6e:73
    PDU revision:      3
    OAM Mode:          active
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
--------------------------------------------------

admin@SwitchA# run show ethernet-oam interface ge-1/1/1
--------------------------------------------------
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          active
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   remote loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:03:35:81
    OUI:               48:6e:73
    PDU revision:      3
    OAM Mode:          passive
```

```
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   supported
    MIB retrieval:     not supported
    Mtu size:          1500

```

- View the statistics information of EFM OAMPDU packets, we can see the number of received Loopback Control OAMPDU packet is 1 on Switch C.

```
admin@SwitchC# run show ethernet-oam statistics interface ge-1/1/1
Packets statistics for interface ge-1/1/1
Packet type                       OAM Tx Count     OAM Rx Count
---------------------------------------------------------------------
OAMInformation                   11365            11372
OAMLoopbackControl               0                1
OAMUnsupported                   0                0
```

Step 3 Stop EFM remote loopback.

```
admin@SwitchC> ethernet-oam remote-loopback stop interface ge-1/1/1
```

Step 4 Verify the Configuration.

- Run the command **run show ethernet-oam**, and you can see that the loopback status is **no loopback** on Switch C and Switch A.

```
admin@SwitchC# run show ethernet-oam
-------------------------------------------------
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          passive
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   no loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:5c:8c:21
    OUI:               48:6e:73
    PDU revision:      3
    OAM Mode:          active
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
-------------------------------------------------
```

- View the statistics information of EFM OAMPDU packets, we can see the number of received Loopback Control OAMPDU packet is 2 on Switch C.

```
admin@SwitchC# run show ethernet-oam statistics interface ge-1/1/1
Packets statistics for interface ge-1/1/1
Packet type                       OAM Tx Count     OAM Rx Count
---------------------------------------------------------------------
OAMInformation                   18770            18792
OAMLoopbackControl               0                2

```

```
7 OAMUnsupported                  0               0
```

Configure Telnet to Access to the Remote Device

Before using the telnet command to connect to a Telnet server, the Telnet client and the Telnet server need to be route reachable, and the Telnet service must be enabled on the Telnet server side.

Run the following command to Telnet to the server via IPv4/IPv6 address or host name:

telnet {<*ip-address*>|<*host-name*>} [<*port-number*>] [**vrf** <*vrf-name*>]

- <*ip-address*>|<*host-name*>: Specifies the IPv4/IPv6 address or host name of a remote system.
- <*port-number*>: Optional. Specifies the TCP port number on which the remote device provides Telnet service. The default port number is 23 which do not need to specified.
- <*vrf-name*>: Optional. Specifies the name of the VRF for the telnet connection. When a VRF name is specified, find the next hop routing information from the specified VRF domain. When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Establish a Telnet connection with a remote device in default VRF.

```
admin@PICOS>  telnet 10.10.51.205 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

- Establish a Telnet connection with a remote device in management VRF.

```
admin@PICOS>  telnet 10.10.51.25 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

Interface Management Configuration Guide

- Ethernet Ports Management Configuration
  - Port Naming Conventions
  - Physical Ethernet Port Configuration
  - Configuring Port Breakout and Merge
    - Overview of Port Breakout
    - 100GE and 40GE
    - 400GE and 200GE
    - 800GE
  - Interface Rate Configuraion
    - Introduction of Interface Rate
    - Configuring the Force Rate of an Interface
    - Configuring the Auto-Negotiation Mode
  - Port Security Configuration
  - CDR Function Configuration
  - Time Domain Reflectometry (TDR)
  - Configuring Port Mapping On S4148 Series Switch
  - 10G-Base-KR Interface Configuration
  - Forwarding Error Correction (FEC)
- Configuring the Loopback Interface
- Layer 3 VLAN Interface Configuration
- Configuring Routed Interface
  - Introduction of Routed Interface
  - Configuration Notes of Routed Interface
  - Configuring Routed Interface and Sub-interface
  - Example for Configuring Routed Interface
- Uplink Failure Detection

Ethernet Ports Management Configuration

- Port Naming Conventions
- Physical Ethernet Port Configuration
- Configuring Port Breakout and Merge
  - Overview of Port Breakout
  - 100GE and 40GE
  - 400GE and 200GE
  - 800GE
- Interface Rate Configuraion
  - Introduction of Interface Rate
  - Configuring the Force Rate of an Interface
  - Configuring the Auto-Negotiation Mode
- Port Security Configuration
- CDR Function Configuration
- Time Domain Reflectometry (TDR)
- Configuring Port Mapping On S4148 Series Switch
- 10G-Base-KR Interface Configuration
- Forwarding Error Correction (FEC)

Port Naming Conventions

The physical interfaces supported by Pica8 switch are shown in Table 1:

Table 1. Physical Interface Supported by Pica8 Switch

Interface Type	Description
GE interface	The GE interface works at the data link layer, provides a maximum transmission rate of 1000 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.
5GE/2.5GE interface	The 5GE/2.5GE interface works at the data link layer, provides a maximum transmission rate of 10 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.
10GE interface	The 10GE interface works at the data link layer, provides a maximum transmission rate of 10 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.
25GE interface	The 25GE interface works at the data link layer, provides a maximum transmission rate of 25 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.
40GE interface	The 40GE interface works at the data link layer, provides a maximum transmission rate of 40 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding. A 40GE optical interface can work as an independent interface or be split into four 10GE optical interfaces.
100GE interface	The 100GE interface works at the data link layer, provides a maximum transmission rate of 100 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding. A 100GE optical interface can work as an independent interface or be split into four 10GE optical interfaces or four 25GE optical interfaces.
200GE interface	The 200GE interface works at the data link layer, provides a maximum transmission rate of 200 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding. A 200GE optical interface can work as an independent interface or be split into four 25GE optical interfaces, two 50GE optical interfaces, four 50GE optical interfaces or two 100GE optical interfaces.
400GE interface	The 400GE interface works at the data link layer, provides a maximum transmission rate of 400 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding. A 400GE optical interface can work as an independent interface or be split into two or four interfaces: • Two 200GE, 100GE or 50GE interfaces. • Four 100GE, 50GE or 25GE interfaces.

800GE interface	The 800GE interface works at the data link layer, provides a maximum transmission rate of 800 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding. An 800GE optical interface can work as an independent interface or be split into two, four or eight interfaces: • Two 400GE, 200GE or 100GE interfaces. • Four 200GE or 1000GE interfaces. • Eight 100GE or 50GE interfaces.

Physical interfaces naming in PICOS are specified as follows:

type-1/1/port

The convention is as follows:

- *type* - The Pica8 device interfaces use the following types:
  - ge - 1G/5G/2.5G Ethernet interface
  - te - 10G/25G Ethernet interface
  - xe - 40G/100G/200G/400G/800G Ethernet interface
- *port* - The port number of Pica8 device. Note that: On the same device, the port number of different types of port starts from 1.

Split Interfaces

The 40G/100G/200G/400G/800G optical interfaces on Pica8 switch can be used as a single interface or split into two or four independent interfaces.

- The 40GE interface can be split into four 10 Gigabit Ethernet interfaces.
- The 100GE interface can be split into four 25 Gigabit Ethernet interfaces or split into four 10 Gigabit Ethernet interfaces. By default, the 100G interface will be split into 4 x 25GE interfaces.
- The 200GE interface can be split into four 25G Gigabit Ethernet interfaces，two 50G Gigabit Ethernet interfaces, four 50G Gigabit Ethernet interfaces or two 100G Gigabit Ethernet interfaces.
- The 400GE interface can be split into four 100 Gigabit Ethernet interfaces, two 200 Gigabit Ethernet interfaces, four 50GE optical interfaces, two 100GE optical interfaces, four 25G Gigabit Ethernet interfaces or two 50G Gigabit Ethernet interfaces.
- The 800GE interface can be split into eight 100GE interfaces, four 200GE interfaces or two 400GE interfaces, and then be reduced into eight 50GE interfaces, four 100GE interfaces, two 200GE interfaces or two 100GE interfaces.

If the port name of the 40G/100G/200G/400G/800G optical interfaces are xe-1/1/n before port breakout; however, after port breakout the port names of the four interfaces are xe-1/1/n.1, xe-1/1/n.2, xe-1/1 /n.3 and xe- 1/1/n.4. For details about port breakout and merge please refer to Configuring Port Breakout and Merge.

Physical Ethernet Port Configuration

You can enable (or disable) the Ethernet port, configure the Ethernet port's MTU, rate-limit, flow control and the duplex mode of optical port.

Shutting Down the Ethernet Port

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the MTU

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 mtu 1200
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Enabling Port Flow Control

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 ether-options flow-control true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring the Duplex Mode of Optical Port as Auto-negotiation Mode

Notes:

- Currently, duplex mode for optical port is only available for the 10 optical port when its port rate set to 1G.
- Duplex mode for optical port currently only supports to configure as auto, i.e. auto-negotiation mode.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 speed 1000
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 duplex auto
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Port Breakout and Merge

- Overview of Port Breakout
- 100GE and 40GE
- 400GE and 200GE
- 800GE

Overview of Port Breakout

NOTEs:

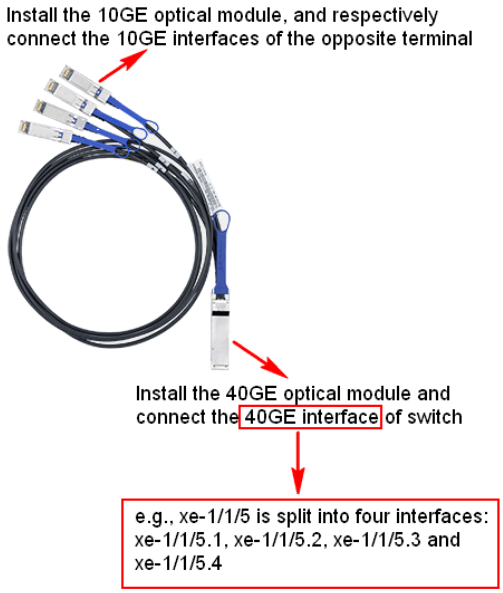
- The 800GE interfaces can be split into two, four, or eight ports. The 400GE and 200GE interfaces can be split into two or four ports, and the 40GE and 100GE interfaces can only be split into four ports.
- You **must** reboot system to make the setting take effect after performing port breakout or merge operation.
- The original interface is illegal after port breakout, and the split interfaces are illegal after port merge. You need to delete related configurations of illegal interfaces before running the command **commit.** Otherwise, error prompts will appear.

An optical interface with high bandwidth can be split into multiple independent low-bandwidth interfaces, which can improve the interface density, reduce the usage cost and increase the network flexibility.

The switch interface can be split into two, four or eight ports. After the interface is split, the configurations and features remain unchanged, while it is named in a different way. For example, the optical interface *xe-1/1/5* is split into four logical interfaces with names of *xe-1/1/5.1~xe-1/1/5.4.*

The split interface can be connected by a common cable or a breakout cable. If interfaces of both terminals are split in the same way, you can use the common cable, and the spilt interfaces are logically connected one to one; if only the interface of one terminal is split, you need use the breakout cable to connect two terminals, as shown in the figure below.

Figure 1. The breakout cable



100GE and 40GE

Overview

NOTEs:

- Due to ASIC limitation, there are some 100GE interfaces on certain platforms do not support port splitting. For details, see Limitation of Port Breakout.

Certain 100GE and 40GE optical interfaces can be used as a single interface or split into four independent interfaces. The 40GE interface can be split into four independent and logical 10 Gigabit Ethernet interfaces. The 100GE interface can be split into four independent and logical 25 Gigabit Ethernet interfaces or four 10 Gigabit Ethernet interfaces.

You can use **set interface gigabit-ethernet** <*port-name*> **breakout true** command to enable port splitting, use **set interface gigabit-ethernet** <*port-name*> **breakout false** command to merge four interfaces into one interface.

Configuring Port Breakout and Port Merge

To configure port breakout for the 40GE or 100GE interfaces of the switch, the procedures are described as below.

Step 1 Split the interface as required.

set interface gigabit-ethernet <*port-name*> **breakout true**

NOTEs:

- When you want to cancel the interface split, use **set interface gigabit-ethernet** <*port-name*> **breakout false** command to restore four interfaces to one interface.
- The interface name is modified after port breakout or merge, that is the original interface does not exist, and you **must** manually delete the configurations associated with the original interfaces before restarting system, to make sure that the configuration file can be loaded normally when system boots up.
- The 100GE interface can be split into four 25G or four 10G Ethernet interfaces. By default, the 100GE interface is split into four 25G Ethernet interfaces. If you want to further split 25G Ethernet interfaces into 10G Ethernet interfaces, configure the speed to 10G through CLI after port breakout. For detailed information of configuring interface speed, see Interface Rate Configuration. **Note**: The speed of the split four interfaces is required to be consistent.

Step 2 Commit the configuration.

commit

Step 3 Enter the Linux shell mode, and restart PICOS to make the setting take effect.

sudo systemctl restart picos

Step 4 Verify the configuration.

For example, split the 40GE interface xe-1/1/25 into four 10GE interfaces and run **run show interface brief** command to view the interface information after system startup.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/25 breakout true
admin@PICOS# commit
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading
startup configuration will fail.
```

```
admin@PICOS# exit
admin@PICOS> start shell sh
admin@PICOS:~$ sudo systemctl restart picos
admin@PICOS> configure
admin@PICOS# run show interface brief
Interface   Management  Status  Flow Control  Duplex  Speed    Description

......
xe-1/1/25.1 Enabled     Down    Disabled      Full    Auto
xe-1/1/25.2 Enabled     Down    Disabled      Full    Auto
xe-1/1/25.3 Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/25.4 Enabled     Up      Disabled      Full    40Gb/s
......
```

400GE and 200GE

Overview

NOTE:

When configuring the split interfaces speed of a certain interface, for N8550-24CD8D, the speed should be consistent; for N9550-64D, N9550-32D and AS9716-32D, the speed can be different.

The 400GE and 200GE optical interface can be used as a single interface or split into two or four independent and logical interfaces. The detailed information is shown as below.

Table 1. Detailed Information of Split Type

Hardware Platform	Panel Interface Type	Optical Module	Split Type
N9550-64D N9550-32D AS9716-32D	400G	400G	4*100G
			2*200G
N8550-24CD8D	400G	400G	4*100G
			2*200G
		200G	4*50G
			2*100G
		100G	4*25G
			2*50G
	200G	200G	4*50G
			2*100G
		100G	4*25G
			2*50G

The speed of certain split interfaces can be further reduced through running command set interface gigabit-ethernet speed. The detailed information is shown below.

Table 2. Detailed Information of the Speed Reduction

Hardware Platform	Panel Interface Type	Optical Module	Split Type	Reduced Speed
N8550-24CD8D	400G	QSPF-DD-SR8-400G	4*100G	4*50G, 4*25G
			2*200G	2*50G, 2*100G

Limitation for N8550-24CD8D

For N8550-24CD8D, it supports thirty-two panel interfaces, which belong to four pipes, that is every eight panel ports (six 200G and two 400G ports) belong to one pipe. For only 18 ports are allowed to be split in one pipe, you need to split interfaces within this limitation. The corresponding relationship **of panel ports and pipes** is shown as below.

Table 2. Corresponding relationships of panel ports and pipes

pipe0	pipe1	pipe2	pipe3
1, 2, 3, 4, 5, 7, 26, 28	6, 8, 13, 15, 17, 19, 30, 32	9, 11, 18, 20, 21, 23, 27, 29	10, 12, 14, 16, 22, 24, 25, 31

Configuring Port Breakout and Port Merge

To configure port breakout for the 400GE interfaces of the switch, take the following steps:.

Step 1 Enable the port breakout function.

set interface gigabit-ethernet <*port-name*> **breakout true**

Step 2 Split the interface as required. The breakout type is different based on switch models.

For N9550-64D, N9550-32D and AS9716-32D, only 400G interface is supported, and you can specify the breakout type as 4 x 100G or 2 x 200G.

set interface gigabit-ethernet <*port-name*> **breakout-type** {**4*100G** | **2*200G**}

For N8550-24CD8D, 400G and 200G interfaces are supported, and you can specify the breakout type as 4 x 100G, 2 x 200G, 4 x 50G, 2 x 100G or 4 x 25G.

set interface gigabit-ethernet <*port-name*> **breakout-type** {**4*100G** | **2*200G** | **4*50G** | **2*100G** | **4*25G**}

NOTEs:

- For 400G interfaces of N8550-24CD8D, when you specify the breakout type as 2*200G or 4*100G:
  - The interface will be split into two 200GE interfaces or four 100GE interfaces with 400G optical module inserted.
  - the interface will be split into two 100GE interfaces or four 50GE interfaces with 200G optical module inserted.
  - The interface will be split into two 50GE interfaces or four 25GE interfaces with 100G optical module inserted.
- For 200G interfaces of N8550-24CD8D:
  - When you specify the breakout type as 2*100G or 4*50G, the interface will be split into two 100GE interfaces or four 50GE interfaces with 200G optical module inserted.
  - When you specify the breakout type as 4*25G, the interface will be split into four 25GE interfaces with 100G optical module inserted.
  - When you specify the breakout type as 2*100G, the interface will be split into two 50GE interfaces with 100G optical module inserted.
- To cancel the interface split, use **set interface gigabit-ethernet** <*port-name*> **breakout false** command to restore the split interfaces into one interface.
- If you enable the breakout function of interface without configuring the breakout-type, the 400GE interface will be split into four 100G Ethernet interfaces and the 200GE interface will be split into four 50G Ethernet interfaces by default.
- The interface name is modified after port breakout or merge, that is the original interface does not exist, and you need to manually delete the configurations associated with the original interfaces before restarting system, to make sure that the configuration file can be loaded normally when system boots up.

Step 3 Commit the configuration.

commit

Step 4 Restart PicOS to make the setting take effect. **Note**: the split interfaces cannot be viewed before restarting PicOS.

sudo systemctl restart picos

Step 5 View the interface information after system startup. You can view the information of split interfaces.

run show interface brief

Configuration Example of Port Breakout

Overview

For N8550-24CD8D, split the 400GE interface into two 200GE interfaces, further reduce the speed of one split interface to 100GE, and view the interface information after system startup.

Procedure

Step 1 Enable the port breakout function.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/48 breakout true
```

Step 2 Specify the breakout type as 2 x 200G.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/48 breakout-type 2*200G
```

Step 3 Commit the configuration.

```
admin@PICOS# commit
```

Step 4 Restart PicOS to make the setting take effect.

```
admin@PICOS# exit
admin@PICOS> start shell sh
admin@PICOS:~$ sudo systemctl restart picos
```

Step 5 Reduce the speed of split interface xe-1/1/48.1 to 100GE.

```
admin@PICOS> configure
admin@PICOS# set interface gigabit-ethernet xe-1/1/48.1 speed 100000
admin@PICOS# commit
```

Verify the configuration

Use the **run show interface brief** command to view the interface xe-1/1/48 information after system startup.

```
admin@PICOS# run show interface brief
Interface       Management Status   Flow Control   Duplex   Speed    Description

--------------  ----------  ------  ------------  ------  -------  ------------------------------

…….           …….      …….     …….        …….    …….

xe-1/1/48.1      Enabled     Up    Disabled      Full    100Gb/s

xe-1/1/48.2      Enabled     Up    Disabled      Full    200Gb/s

xe-1/1/49       Enabled     Down    Disabled      Full    Auto
```

```
13
14 ..... ..... . ..... ..... ..... .....
```

800GE

Overview

The 800GE optical interface can be used as a single interface or split into multiple independent and logical interfaces. The speed of split interfaces can be further reduced through running command **set interface gigabit-ethernet speed**. The detailed information is shown below.

Table 1. Detailed Information of Split Type and Speed Reduction

Hardware Platform	Panel Interface Type	Optical Module	Split Type	Reduced Speed
N9600-64OD	800G	800G	8*100G	8*50G
			4*200G	4*100G
			2*400G	2*200G, 2*100G

Configuration Notes and Constraints

When configuring the port breakout and port merge, pay attention to the following notes:

- Currently, only the platform of N9600-64OD supports 800GE optical interfaces.
- After you split an interface into 8 x 100G, another port in the same group cannot be split or can only be split into 2 x 400G due to chip limitations. For example, xe-1/1/1 and xe-1/1/2 are in a group, if you split the interface xe-1/1/1 into 8 x 100G, the interface xe-1/1/2 cannot be split or can only be split into 2 x 400G.
- Certain 800G optical modules do not support certain split types and speed reduction for their own limitations. For detailed information, contact the FS support staff.
- If you enable the breakout function of interface without configuring the breakout-type, the 800GE interface will be split into four 200G Ethernet interfaces by default.
- The interface name is modified after port breakout or merge, and the original interface does not exist. To make sure that the configuration file can be loaded normally when system boots up, you need to manually delete the configurations associated with the original interfaces before restarting system.
- To cancel the interface split, use the command **set interface gigabit-ethernet** <*port-name*> **breakout false** to restore the split interfaces into one interface.

Configuring Port Breakout and Port Merge

To configure the port breakout for the 800GE interfaces, take the following steps:

Step 1 Enable the port breakout function.

set interface gigabit-ethernet <*port-name*> **breakout true**

Step 2 Split the interface as needed. You can specify the breakout type as 8 x 100G, 4 x 200G or 2 x 400G.

set interface gigabit-ethernet <*port-name*> **breakout-type** {**2*400G** | **4*200G | 8*100G**}

Step 3 Commit the configuration.

commit

Step 4 Restart PICOS to make the setting take effect. **NOTE**: the split interfaces cannot be viewed before restarting PICOS.

sudo systemctl restart picos

Step 5 View the interface information after system startup. You can view the information of split interfaces.

run show interface brief

Configuration Example of Port Breakout

Overview

For N9600-64OD, split the 800GE interface into two 400GE interfaces, and further reduce the speed of one split interface to 200GE. You can view the interface information after system startup.

Procedure

Step 1 Enable the port breakout function.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/48 breakout true
```

Step 2 Specify the breakout type as 2 x 400G.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/48 breakout-type 2*400G
```

Step 3 Commit the configuration.

```
admin@PICOS# commit
```

Step 4 Restart PICOS to make the setting take effect.

```
admin@PICOS# exit
admin@PICOS> start shell sh
admin@PICOS:~$ sudo systemctl restart picos
```

Step 5 Reduce the speed of split interface xe-1/1/48.1 to 200GE.

```
admin@PICOS> configure
admin@PICOS# set interface gigabit-ethernet xe-1/1/48.1 speed 200000
admin@PICOS# commit
```

Verifying the configuration

Use the command **run show interface brief** to view the interface xe-1/1/48 information after system startup.

```
admin@PICOS# run show interface brief
Interface       Management Status   Flow Control   Duplex   Speed    Description

--------------  ----------  ------  ------------  ------  -------  ------------------------------

…….           …….      …….     …….        …….    …….

xe-1/1/48.1      Enabled     Up    Disabled      Full    200Gb/s

xe-1/1/48.2      Enabled     Up    Disabled      Full    400Gb/s

xe-1/1/49       Enabled     Down    Disabled      Full    Auto

……           …….        ……     ……          ……   ……

```

Interface Rate Configuraion

- Introduction of Interface Rate
- Configuring the Force Rate of an Interface
- Configuring the Auto-Negotiation Mode

Introduction of Interface Rate

Interface rate can be configured in the two modes: force rate (non-auto-negotiation mode) and auto-negotiation mode.

> **NOTE:**
>
> - Interfaces at both ends of a link SHOULD work in the same auto-negotiation mode. Otherwise, the interfaces may not be able to communicate with each other.
> - The 2.5G/5G RJ45 ports don't support to set the force speed by using **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command. Users can configure auto-negotiation mode to auto-negotiate the interface rate for these ports, together with the optional **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** <*auto-speed*> command to manually specify the auto-negotiation rate range.

Force Rate (Non-auto-negotiation Mode)

If you want to use a specific interface rate for communication rather than auto-negotiate the interface rate, you can configure the force rate of the interface.

You can configure the force rate of an interface by using the **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command.

> **NOTE:**
>
> When configuring the force rate of an interface, make sure that the interface rates configured on the two ends of the link are the same.

Instructions for the switch interface rate configuration:

1. 1G RJ45 port: The interface rate can be configured to 100M, 10M or auto. By default, the interfaces work in auto-negotiation mode.
2. 1G optical port: The interface rate can be configured to 1000M or auto. By default, the interfaces work in auto-negotiation mode.
3. 10G RJ45 port: The interface rate can be configured to 100M or auto. By default, the interfaces work in auto-negotiation mode.
4. 10G optical port:

- When a 10G optical module is inserted, the interface rate can be configured to 10G or 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 10G.
- When a 1G optical module is inserted, the interface rate can be configured to 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 1G.

5. 40G optical port: The interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G or 1G.
6. 100G optical port:

- When a 100G optical module is inserted, the interface rate can be configured to 100G or 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 25G or 10G.
- When a 40G optical module is inserted, the interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G.

7. 200G optical port:

- When a 200G optical module is inserted, the interface rate can be configured to 200G,100G or 50G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 100G or 50G.
- When a 100G optical module is inserted, the interface rate can be configured to 100G,50G or 25G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 50G or 25G.

8. 400G optical port:

- When a 400G optical module is inserted, the interface rate can be configured to 400G, 200G or 100G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 200G or 100G.
- When a 200G optical module is inserted, the interface rate can be configured to 200G,100G or 50G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 100G or 50G.
- When a 100G optical module is inserted, the interface rate can be configured to 100G, 50G or 25G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 50G or 25G.

9. 800G optical port: Only 800G optical module can be inserted, and the interface rate can be configured to 800G, 400G, 200G or 100G. When no force rate is configured, the interface recognizes the interface rate of itself as 800G.

- If the interface configured interface split, the split interface rate can be configured to 400G, 200G or 100G.
- The speed of split interfaces can be further reduced by running the command **set interface gigabit-ethernet speed**. The reduced speed of split interfaces: 400G supports 200G and 100G; 200G supports 100G; 100G supports 50G.

Auto-negotiation Mode

When the ports of the switch in the network support multiple transmission rate, the user can configure auto-negotiation mode to auto-negotiate the interface rate. The devices at both ends of the link exchange interactive messages with the device capability, thus automatically negotiate the optimal interface rate of the interfaces at both ends of the link.

Use the **set interface gigabit-ethernet**<*interface-name*> **speed auto** command to enable the auto-negotiation mode of the interface.

Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode. By default, these interfaces work in auto-negotiation mode. In auto-negotiation mode the ports negotiate any rate supported by the two devices. To enable non-auto-negotiation mode, you can configure the force rate of the interface by using **set interface gigabit-ethernet**<*interface-name*> **speed** <*speed*> command.

If the negotiated interface rate is not the required value, you can use the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate to make the interface negotiate the rate within the specified range. The auto-negotiation rates configured on the interfaces must have an intersection at both ends of the link.

Use **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** multiple times to set multiple negotiation rates.

Example 1:

The following commands configure multiple auto-negotiation rates on interface ge-1/1/1 to specify the range of auto-negotiation rate to 1000M, 100M and 10M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 1000
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 100
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 10
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

Example 2:

The following commands configure one auto-negotiation rate on interface ge-1/1/1 to specify the range of auto-negotiation rate to 1000M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 1000
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

NOTE:

- Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode and auto-negotiation rate.
- Run the **set interface gigabit-ethernet**<*interface-name*>**speed auto** command to configure the Ethernet interface to work in auto-negotiation mode before using the **set interface gigabit-ethernet**<*interface-name*>**auto-speeds** command to manually specify the auto-negotiation rate.
- In auto-negotiation mode, the device automatically negotiates the duplex mode of the interface while negotiating the interface rate.

Configuring the Force Rate of an Interface

This section describes how to configure the force rate of an interface.

Procedure

- Configure the force rate of an interface.

  set interface gigabit-ethernet<*interface-name*> **speed** <*speed*>

Configuration Example

- Configure the force rate of the Te-1/1/5 port to 100 M.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/5 speed 100
admin@Xorplus# commit
```

Verify the Configuration

- Use **run show interface gigabit-ethernet** command to view the current interface status information of te-1/1/5 interface. Check the **Speed** and **Auto-negotiation** field in the command output. **Auto-negotiation** field is **Disabled** when in non-auto-negotiation mode.

```
admin@XorPlus# run show interface gigabit-ethernet te-1/1/5
Physical interface: te-1/1/5, Enabled, error-discard False, Physical link is Up
Interface index: 5, SFP type: unknown, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 1Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Link fault signaling  ignore local fault:false, ignore remote fault:false
force up mode:false
Precision Time Protocol mode:none
Current address: 48:6e:73:01:00:bb, Hardware address: 48:6e:73:01:00:bb
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 544 bits/sec, 0 packets/sec
  Input Packets.....................0
  Output Packets....................9149
  Input Octets......................0
  Output Octets.....................1125327
```

Configuring the Auto-Negotiation Mode

This section describes how to configure the auto-negotiation mode.

- Procedure
- Configuration Example
- Verify the Configuration

Procedure

Step1 Enable auto-negotiation mode.

set interface gigabit-ethernet<*interface-name*> **speed auto**

> **NOTE:**
>
> Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode and to set auto-negotiation rate.

Step2 Configure the auto-negotiation rate of Ethernet interfaces in auto-negotiation mode.

set interface gigabit-ethernet <*interface-name*> **auto-speeds** <*auto-speed*>

Configuration Example

Step1 Enable auto-negotiation mode.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

> **NOTE:**
>
> Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode and to set auto-negotiation rate.

Step2 Configure the auto-negotiation rate of ge-1/1/1.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 100
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 10
```

Verify the Configuration

- Use **run show interface gigabit-ethernet ge-1/1/1** command to view the current interface status information of ge-1/1/1 interface. Check the **Speed** and **Auto-negotiation** field in the command output.

```
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard False, Physical link is Up
Interface index: 5, SFP type: unknown, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 1Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Enabled, Advertised speed modes: 10M,100M
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Link fault signaling  ignore local fault:false, ignore remote fault:false
force up mode:false
Precision Time Protocol mode:none
Current address: 48:6e:73:01:00:bb, Hardware address: 48:6e:73:01:00:bb
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 544 bits/sec, 0 packets/sec
  Input Packets.....................0
  Output Packets....................9149
  Input Octets......................0
  Output Octets.....................1125327
```

Port Security Configuration

Port security function limits the number of MAC addresses that can access the switch port, preventing illegal users from communicating with the network through the switch interface, thus enhancing the security of network resources.

The dynamic MAC address learned by the secure interface is converted into secure MAC address, and the maximum number of secure MAC addresses is allowed to be configured. When the number of learned MAC addresses exceeds the MAC limit, a violation action is triggered to protect the system, which can be configured by the user to shut down the port or discard packets with new source MAC addresses.

NOTE:
When configuring port security, follow the guidelines and restrictions described below:

- By enabling the port security function, the dynamic MAC address table entries learned previously on the secure interface will be deleted automatically and the static MAC address table entry configured previously will be prompted to manually delete.
- Port security and static MAC configurations on the same interface are mutually exclusive.
- Port security does not support to configure on a LAG interface.
- Make sure MAC learning is enabled before enabling port security on the same interface. (By default, MAC learning is enabled.)
- Executing the command "**run clear MAC address table all**" will clear only the dynamic secure MAC addresses, but not clear static secure MAC and sticky secure MAC.
- When the secure port goes Down and Up, the system clears only dynamic secure MAC, but not clear static secure MAC and sticky secure MAC.
- A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.
- For dynamic security MACs, you can move them to any other port; however, for sticky security MACs, learning on any other port is not supported unless statically configured.
- The new learned MAC addresses will temporarily occupy the system MAC address table resources when it reaches the MAC limit. In this case, if the interface still learns a large number of MAC addresses, it may cause the device to temporarily fail to learn the new MAC address.

Enabling Port Security

When port security is enabled, the dynamic MAC address table entries learned previously on the secure interface will be deleted automatically and the static MAC address table entry configured previously will be prompted to manually delete.

After port security is enabled, the dynamic MAC addresses learned on the secure interface will be changed to a dynamic secure MAC address.

When port security is disabled, all the secure MAC addresses on the interface will be deleted, and the port will need to re-learn the MAC address on the port.

The following example enables port security on interface ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security
admin@XorPlus# commit
Commit OK.
Save done.
```

Three Types of Secure MAC

There are three types of secure MAC address on a secure port: Dynamic Secure MAC, Static Secure MAC and Sticky Secure MAC.

1. Dynamic Secure MAC

Dynamic secure MAC is the MAC address dynamically learned on the secure port.

When the secure port goes Down and Up, or device reboots/restarts, the dynamic secure MAC addresses are lost and needs to be re-learned.

Dynamic secure MAC addresses will be aged out by the following MAC aging time CLI command.

```
admin@XorPlus# set interface ethernet-switching-options mac-table-aging-time 100
admin@XorPlus# commit
Commit OK.
Save done.
```

2. Static Secure MAC

Static secure MAC addresses are configured by the user with the following CLI command.

The configuration will not be lost when the switch is rebooted/restarted, or port goes down and up.

Static secure MAC addresses do not age.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:23 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:24 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:25 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:26 vlan 1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-address 00:00:23:23:23:27 vlan 1
admin@XorPlus# commit
```

```
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:23:23:23:23 static ge-1/1/1
1 00:00:23:23:23:24 static ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
1 00:00:23:23:23:26 static ge-1/1/1
1 00:00:23:23:23:27 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

3. Sticky Secure MAC

When sticky function is enabled on the secure port, the system changes the dynamic secure MAC to sticky secure MAC.

Port security with sticky MAC addresses retains dynamically learned MAC addresses when the port goes down and restores the MAC addresses when the link is up.

Sticky secure MAC addresses also do not age.

NOTE:

- After a device reboots/restarts, sticky secure MAC addresses are lost and need to be re-learned.
- Disabling the sticky function converts the sticky secure MAC addresses on the current interface to dynamic secure MAC addresses.

For example, enable sticky function on secure port ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security sticky true
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
admin@XorPlus#
```

In **run show port-security address**, the MAC type of the sticky secure MAC is displayed as sticky; however, in **run show MAC address table**, the MAC type of the sticky secure MAC is displayed as static.

For example,

```
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 sticky ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s

admin@Xorplus# run show mac-address table
Total entries in switching table:   2
Static entries in switching table:  2
Dynamic entries in switching table: 0

VLAN   MAC address    Type      Age    Interfaces      User
----      -----------------    ---------    ----    ----------------   ----------
1        00:00:11:11:11:11 static      300    ge-1/1/1       xorp
1        00:00:23:23:23:25 static      300    ge-1/1/1       xorp
```

Configuring the Maximum Number of Secure MACs

The MAC limit number is used to limit the number of secure MACs on the interface, including the number of dynamic secure MAC and manually configured secure static MAC. If sticky is enabled, MAC limit includes sticky secure MAC and secure static MAC.

A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-limit 5
admin@XorPlus# commit
Commit OK.
Save done.
```

```
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:11:11:11:12 dynamic ge-1/1/1
1 00:00:11:11:11:13 dynamic ge-1/1/1
1 00:00:11:11:11:14 dynamic ge-1/1/1
1 00:00:11:11:11:15 dynamic ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

Configuring Port Security Violation Mode on a Port

Violation mode can be configured for the system to take a protective action when the number of learned MAC addresses exceeds the MAC limit on the secure port, as one of the following four:

- **protect**: Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit. This is the default value.
- **restrict**: Discards packets with new source MAC addresses and generates a warning syslog message when the number of learned MAC addresses exceeds the limit.
- **shutdown**: Shuts the interface down, sets the interface status toerror-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. User can recover the port with the **run clear port-security port-error** command.
- **shutdown-temp**: Shuts the interface down temporarily, sets the interface status to error-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. After 20 seconds (default), the interface comes up. The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is configured to **shutdown-temp**.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/33 port-security violation ?
Possible completions:
  protect                      Drop packets with unknown source addresses
  restrict                     Drop packets with unknown source addresses and log violation
  shutdown                    Disable interface
  shutdown-temp               Disable interface temporarily (20 seconds by default)

admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security violation restrict
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Port Security Auto-recovery Time

When the port security violation mode is configured to shutdown-temp, user can configure the recovery interval with the command below.

```
admin@XorPlus# set interface ethernet-switching-options port-error-discard timeout 30
admin@XorPlus# commit
Commit OK.
Save done.
```

Recovering the Port in Error-discard

When the port security violation mode is configured to **shutdown**, the port will be set to error-discard state after detecting a violation. User can recover the port with the following command.

```
admin@Xorplus# run show interface gigabit-ethernet ge-1/1/23
Physical interface: ge-1/1/23, Enabled, error-discard True(Port Security), Physical link is Down
Interface index: 23, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1518, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Enabled, Advertised speed modes: 10M,100M,1G
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Precision Time Protocol mode:none
Current address: 20:04:0f:01:63:4a, Hardware address: 20:04:0f:01:63:4a
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
```

```
  Input Packets.........................42
  Output Packets........................31
  Input Octets..........................4781
  Output Octets.........................4545

admin@XorPlus# run clear port-security port-error interface gigabit-ethernet ge-1/1/33
Clear done.
```

Configuring Port Security Block Mode

Port security can be configured to take one of five block actions:

- **all**: Discards all the packets in egress direction of the port.
- **broadcast**: Discards only the broadcast packets in egress direction of the port.
- **multicast**: Discards only the multicast packets in egress direction of the port.
- **uni-multi-cast**: Discards both the unknown unicast packets and multicast packets in egress direction of the port.
- **unicast**: Discards only the unknown unicast packets in egress direction of the port.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/33 port-security block ?
Possible completions:
  all                           Block broadcast and unknown addresses
  broadcast                     Block broadcast address
  multicast                     Block unknown multicast addresses
  uni-multi-cast                Block unknown uni/multi cast addresses
  unicast                       Block unknown unicast addresses

admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security block broadcast
admin@XorPlus# commit
Commit OK.
Save done.
```

Displaying Port Security Settings

To display port security settings, enter this command:

```
admin@Xorplus# run show port-security brief
Secure Port    MaxMacLimit    CurrentAddr    ViolationCount    Action
-------------------------------------------------------------------------------------------------------------------
ge-1/1/22      2              0              0                 restrict
ge-1/1/23      1              0              0                 shutdown-temp
ge-1/1/34      1              0              0                 protect

admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ----------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:23:23:23:26 static ge-1/1/1
1 00:00:23:23:23:27 static ge-1/1/1
-----------------------------------------------------
MAC age time :100s

admin@Xorplus# run show port-security interface
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/23
---------------------------------------
Port Security               : enabled
```

```
Violation action            : shutdown-temp
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

Disabling Port Security

To disable port security, enter this command:

```
admin@XorPlus# delete interface gigabit-ethernet ge-1/1/1 port-security
Deleting:
port-security {
mac-limit: 5
violation: "restrict"
mac-address 00:00:23:23:23:23 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:24 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:25 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:26 {
vlan 1 {
}
}
mac-address 00:00:23:23:23:27 {
vlan 1 {
}
}
sticky: true
block: "broadcast"
}
OK
admin@XorPlus# commit
Commit OK.
Save done.
```

CDR Function Configuration

Clock and Data Recovery (CDR) is a process that is dependent upon a clock signal synchronous with the data flow. When a data flow arrives at the receiver, it is sent without additional clocking information, the receiver generates a clock from an approximate frequency reference, and then phase-aligns the clock to the transitions in the data flow with a phase-locked loop (PLL). Data distortion, noise, and jitter on the incoming data can be reduced if the CDR technology is used for data recovery from the transmission channel.

> **NOTEs:**
>
> - CDR function can only be configured on the 800G, 400G, 200G, 100G or 40G optical module interface and the split interfaces broke out from them.
> - The CDR configurations of split interfaces which broke out from the 800G, 400G, 200G, 100G or 40G optical module interface should be the same.

Procedure

- Use the following command to disable or enable the CDR function.

  set interface gigabit-ethernet <*interface-name*> **cdr** [**true | false**]

  The default setting is **true**. The command takes effect immediately after committing.

Configuration Example

- Enable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr true
admin@Xorplus# commit
```

- Disable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr false
admin@Xorplus# commit
```

Time Domain Reflectometry (TDR)

- Introduction
- Configuration Notes
- Configuring TDR Function
  - Procedure
  - Configuration Example

Introduction

Time Domain Reflectometry (TDR) technology is used to detect faults in metallic cables that are connected to the Ethernet electrical interface of a switch. When a pulse signal is transmitted through a cable, part of the energy is reflected back if it encounters a cable end or a fault point. The TDR algorithm measures the time that a pulse travelling through the cable, reaching the fault point, and returning, and then converts the measured time into a distance.

Assume the distance between the interface and the fault point is **Distance**, the time interval from the pulse signal being sent to when it is received is **T**, and the transmission rate of the pulse signal in the cable is **V**. Then the formula for calculating the distance from the fault point to the switch interface is as follows:

Distance = (V x T) / 2

The TDR test command detects the cable connected to the Ethernet electrical interface and display the detection result:

- When the cable is not faulty, the Pair length displayed refers to the total length of the cable.
- When the cable is faulty, the Pair length displayed is the length from the interface to the fault point in the cable.

Configuration Notes

When employing TDR test on a switch interface, pay attention to the following points:

- TDR test is only used on the Ethernet electrical interface but not suitable for the Optical interface.
- As there is a certain error (refers to the Pair length column in the test results) in the TDR test, so the results are for reference only.
- The recommended cable length for TDR test is less than 100m.
- The interface on which the TDR test is running flaps for a short period of time, this may cause service interruption for a short time.
- Make sure that the interface is enabled when running TDR test.
- The time consumed for TDR test is different on different platforms, from 2 to 8 seconds.
- The combo interface of the switch does not support the TDR function.

Configuring TDR Function

Procedure

- Run the following command to start the TDR cable test and check the test result from the displayed information.

  run show interface diagnostics tdr *<interface-name>*

  After the command is issued, the test result will be displayed. The time consumed for TDR test is different on different platforms, from 2 to 8 seconds.

Configuration Example

- Run the following command to start the TDR cable test. The following example shows the cable length (Pair length) is approximately 31 meters long with a possible error of +/- 10 meters.. All four pairs are working fine (Pair status).

```
admin@Xorplus# run show interface diagnostics tdr ge-1/1/1
Interface  Local pair Pair length(meter) Remote pair Pair status
---------- ---------- ------------------ ----------- -----------
ge-1/1/1   Pair A     31   +/- 10        Pair A      OK
           Pair B     31   +/- 10        Pair B      OK
           Pair C     31   +/- 10        Pair C      OK
           Pair D     30   +/- 10        Pair D      OK
```

Table 1. Description of the run show interface diagnostics tdr output

Item	Description
Interface	Indicates the interface name of the switch.
Local pair	Local four pairs.

Item	Description
Pair length(meter)	Displays the length and error of the cable pair in meters. • When the pair is not faulty, the Pair length in the displayed message refers to the total length of the pair. • When the pair is faulty, the Pair length in the displayed message is the length from the interface to the fault point in the cable.
Remote pair	Remote four pairs.
Pair status	The pair status could be "**OK**", "**OPEN**", "**SHORT**", "**OPENSHORT**", "**CROSSTALK**" or "**N/A**". • **OK**: indicates the link is up, the cable are working fine. • **OPEN**: indicates an open circuit, meaning a broken wire or maybe cable unplugged. • **SHORT**: indicates there is a short circuit on the cable. • **N/A**: indicates the port does not support TDR test.

Configuring Port Mapping On S4148 Series Switch

This document is only available for S4148 series switch.

- Procedure
- Configuration Example
- Verify the configuration

The six interfaces of QSFP+ and QSFP28 on the switch, with port numbers from 25 to 30, form an interface group. You can configure the port mapping mode of this interface group as required, the value could be **6 x 40G** or **4 x 100G**.

- **6 x 40G**: This is the default port mapping mode. In this mode, all the six interfaces work at 40G mode. The interface names are xe-1/1/1, xe-1/1/2, xe-1/1/3, xe-1/1/4, xe-1/1/5 and xe-1/1/6.
- **4 x 100G**: In this port mapping mode, the four QSFP28 interfaces numbering 25, 26, 29 and 30 work at 100G mode and the other two QSFP+ interfaces numbering 27 and 28 are unavailable. In this mode, the interface names of the four QSFP28 interfaces are xe-1/1/1, xe-1/1/2, xe-1/1/3 and xe-1/1/4.

Procedure

- From the Linux shell prompt, run the following command.

```
admin@XorPlus:~$ sudo picos_boot port-layout
Configure the front panel QSFP interfaces port map options:
    [1]  6x40G_QSFP    * default
    [2]  4x100G_QSFP
Enter your choice(1,2):
```

Type the option number at the "**Enter your choice(1,2):**" prompt and press Enter to select the port mapping mode.

NOTE:

- Run this command in Linux shell.
- To run this command, you need root privileges.
- The default setting is 6x40G_QSFP.
- After changing the port mapping mode, you need to restart PICOS to make the setting take effect.
- Manually remove the user configuration files **/pica/config/pica_startup.boot** and **/pica/config/pica.conf** after changing port mapping mode and before restarting PICOS. Be cautious that all the user configurations will be lost after these operations. We suggest you backup the configuration file before proceeding with these operations.
- Hardware limitation – if power cycle the switch, wait for 10 - 30 seconds before power on.

Configuration Example

The example below shows the steps for configuring the port mapping mode as 4 x 100G.

Step1 From the Linux shell prompt, run **picos_boot port-layout** command to configure the port mapping mode to 4x100G.

```
admin@XorPlus:~$ sudo picos_boot port-layout
Configure the front panel QSFP interfaces port map options:
    [1]  6x40G_QSFP    * default
    [2]  4x100G_QSFP
Enter your choice(1,2):
```

Step2 Type "**2**" and press Enter to set the port mapping mode to 4x100G_QSFP. By default, the port mapping mode is set to 6x40G_QSFP.

Step3 Manually remove the user configuration files.

After changing the port mapping mode and before restarting PICOS, you need to manually remove the user configuration files **/pica/config/pica_startup.boot** and **/pica/config/pica.conf**.

```
admin@XorPlus:~$ sudo rm /pica/config/pica_startup.boot
admin@XorPlus:~$ sudo rm /pica/config/pica.conf
```

Step4 After changing the port mapping mode, you need to restart PICOS to make the setting take effect.

```
admin@XorPlus:~$ exit
admin@XorPlus> request system reboot
```

Verify the configuration

- After the system boots, run **run show interface brief** command to view the interface information.

In 4x100G_QSFP mode, we can see that the four QSFP28 interfaces numbering 25, 26, 29 and 30 are working at 100G, and the other two QSFP+ interfaces numbering 27 and 28 are unavailable. The interface names of the four QSFP28 interfaces are xe-1/1/1, xe-1/1/2, xe-1/1/3 and xe-1/1/4.

```
admin@XorPlus# run show interface brief
Interface     Management  Status  Flow Control  Duplex  Speed    Description
----------    ----------  ------  ------------  ------  -------  ------------------------------
xe-1/1/1(25)   Enabled     Up      Disabled      Full    Auto
xe-1/1/2(26)   Enabled     Down    Disabled      Full    Auto
xe-1/1/3(29)   Enabled     Down    Disabled      Full    Auto
xe-1/1/4(30)   Enabled     Down    Disabled      Full    Auto
```

10G-Base-KR Interface Configuration

NOTEs:

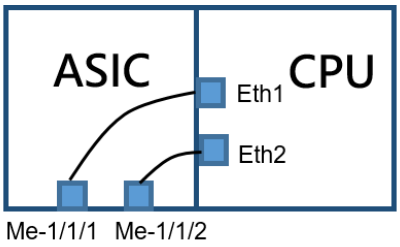
- Only AS7726-32X and AS7326-56X support to disable the 10G-Base-KR ports. By default, they are disabled on AS7726-32X and AS7326-56X.
- On other platforms, by default, the two 10G-Base-KR ports are two 10G-KR management ports linked to CPU.
- If you change the mapping mode of a 10G Base KR port, the port name will also change. Therefore, before changing the mapping mode of the 10G Base KR port, you need to manually delete or modify the configuration of the unavailable interfaces (such as me-1/1/1, me-1/1/2, te-1/1/1, or te-1/1/2) to ensure that the configuration file can be loaded properly upon system restart.
- There is a limitation when enabled the 10G-Base-KR ports as either front panel ports or management ports, namely:
  - On AS7726-32X and N8550-32C, port xe-1/1/32 is not allowed to be split into four Gigabit Ethernet ports.
  - On AS7326-56X and N8550-48B8C, port xe-1/1/8 is not allowed to be split into four Gigabit Ethernet ports.
- The interface rate of the two Me ports can only support auto-negotiation mode.

Introduction

AS7726-32X, AS7326-56X, N8550-48B8C and N8550-32C have two 10G-Base-KR ports (10G-KR) on the front panel to support additional high-speed link between CPU and ASIC (switch chip). PICOS supports to configure the two 10G-Base-KR ports as two 10G SFP+ front panel data ports or they can be configured to provide additional high speed links between the switch CPU and ASIC.

When configured as front panel data ports, they can be used as normal SFP+ port. As a data port, the interface name becomes *Te-1/1/m*. As shown in **Figure 1**, when configured as two 10G-KR ports, the ports are linked to two management ports eth1 and eth2 on the CPU with 10G bandwidth, and the port name becomes *Me-1/1/n* (Management Ethernet port) under PICOS CLI. This alllows the management traffic and data traffic through the *Me-1/1/n* ports can be processed by eth1 and eth2 ports on the CPU.

Figure 1. 10G-KR ports link between CPU and ASIC



Supported Platforms

Currently only AS7726-32X, AS7326-56X, N8550-48B8C and N8550-32C switches have the 10G-Base-KR ports which can be configured as two 10G SFP+ data ports on the front panel or as two 10G-KR management ports linked to CPU. By default, 10G-Base-KR ports are disabled.

Configuration

This section describes how to configure the two 10G-Base-KR ports as front panel ports or management ports linked to CPU.

Configuring as the Management Port

- From the Linux shell prompt, run **sudo picos_boot management-port-mapping** command to configure the 10G-Base-KR ports as two 10G-KR management ports linked to CPU. The option ***[3] No me Port(s)*** indicates that the 10G-Base-KR ports are disabled. Only AS7726-32X and AS7326-56X support to disable the 10G-Base-KR ports.

```
admin@PICOS:~$ sudo picos_boot management-port-mapping
    [1]  To Host CPU
    [2]  To Front Panel
    [3]  No me Port(s)      * default
Enter your choice(1,2,3):1

 To Host CPU is selected.
Please restart the PICOS service
```

- Restart PICOS to make the configuration take effect.

```
admin@Xorplus:~$ exit
admin@Xorplus> request system reboot
```

- We can use **run show interface brief** to check the interface configuration information.

Take AS7726-32X as an example, we can see that the port name of the last two 10G-Base-KR ports are me-1/1/1 and me-1/1/2. They are two 10G-KR management ports linked to CPU.

```
admin@Xorplus# run show interface brief
Interface   Management  Status  Flow Control  Duplex  Speed    Description
----------  ----------  ------  ------------  ------  -------  ------------------------------
xe-1/1/1    Enabled     Down    Disabled      Full    Auto
xe-1/1/2    Enabled     Down    Disabled      Full    Auto
xe-1/1/3    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/4    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/5    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/6    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/7    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/8    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/9    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/10   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/11   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/12   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/13   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/14   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/15   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/16   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/17   Enabled     Down    Disabled      Full    Auto
xe-1/1/18   Enabled     Down    Disabled      Full    Auto
xe-1/1/19   Enabled     Down    Disabled      Full    Auto
xe-1/1/20   Enabled     Down    Disabled      Full    Auto
xe-1/1/21   Enabled     Down    Disabled      Full    Auto
xe-1/1/22   Enabled     Down    Disabled      Full    Auto
xe-1/1/23   Enabled     Down    Disabled      Full    Auto
xe-1/1/24   Enabled     Down    Disabled      Full    Auto
xe-1/1/25   Enabled     Down    Disabled      Full    Auto
xe-1/1/26   Enabled     Down    Disabled      Full    Auto
xe-1/1/27   Enabled     Down    Disabled      Full    Auto
xe-1/1/28   Enabled     Down    Disabled      Full    Auto
xe-1/1/29   Enabled     Down    Disabled      Full    Auto
xe-1/1/30   Enabled     Down    Disabled      Full    Auto
xe-1/1/31   Enabled     Down    Disabled      Full    Auto
xe-1/1/32   Enabled     Down    Disabled      Full    Auto
me-1/1/1(33)  Enabled     Up      Disabled      Full    Auto
me-1/1/2(34) Enabled     Up      Disabled      Full    Auto
```

Under Linux shell, you can see the two ports eth1 and eth2 in addition to the management port eth0 as the **ifconfig -a** command shows below. Under PICOS CLI, the Me ports are bound to the two management ports eth1 and eth2 on CPU. Applications of Linux including PICOS can access (read/write) eth1 and eth2. For example, port configurations such as trunk VLANs can be applied to Me ports.

```
root@Xorplus:/home/admin# ifconfig -a
dummy0    Link encap:Ethernet  HWaddr 72:c9:69:6f:35:2d
          BROADCAST NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr b8:6a:97:8a:77:68
          inet addr:10.10.51.60  Bcast:10.10.51.255 Mask:255.255.255.0
          inet6 addr: fe80::ba6a:97ff:fe8a:7768/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6923 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:494847 (483.2 KiB)  TX bytes:24437 (23.8 KiB)
          Interrupt:16

eth1      Link encap:Ethernet  HWaddr b8:6a:97:8a:77:69
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2      Link encap:Ethernet  HWaddr b8:6a:97:8a:77:6a
          BROADCAST MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

Configuring as Front Panel Ports

- From the Linux shell prompt, run **sudo picos_boot management-port-mapping** command to configure the 10G-Base-KR ports as 10G SFP+ data ports on the front panel.

```
admin@PICOS:~$ sudo picos_boot management-port-mapping
    [1]  To Host CPU        * default
    [2]  To Front Panel
    [3]  No me Port(s)
Enter your choice(1,2,3):2

To Front Panel is selected.
Please restart the PICOS service
```

- Restart PICOS to make the configuration take effect.

```
admin@Xorplus:~$ exit
admin@Xorplus> request system reboot
```

- We can use **run show interface brief** to check the interface configuration information.

Take AS7726-32X as an example, we can see the last two 10G-Base-KR ports are configured as two 10G SFP+ ports and the port names are te-1/1/1 and te-1/1/2. When configured as the front panel ports, the 10G-Base-KR ports can be used as normal 10G SFP+ ports.

```
admin@Xorplus# run show interface brief
Interface   Management  Status  Flow Control  Duplex  Speed    Description
----------  ----------  ------  ------------  ------  -------  ------------------------------
xe-1/1/1    Enabled     Down    Disabled      Full    Auto
xe-1/1/2    Enabled     Down    Disabled      Full    Auto
xe-1/1/3    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/4    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/5    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/6    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/7    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/8    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/9    Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/10   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/11   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/12   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/13   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/14   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/15   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/16   Enabled     Up      Disabled      Full    40Gb/s
xe-1/1/17   Enabled     Down    Disabled      Full    Auto
xe-1/1/18   Enabled     Down    Disabled      Full    Auto
xe-1/1/19   Enabled     Down    Disabled      Full    Auto
xe-1/1/20   Enabled     Down    Disabled      Full    Auto
xe-1/1/21   Enabled     Down    Disabled      Full    Auto
xe-1/1/22   Enabled     Down    Disabled      Full    Auto
xe-1/1/23   Enabled     Down    Disabled      Full    Auto
xe-1/1/24   Enabled     Down    Disabled      Full    Auto
xe-1/1/25   Enabled     Down    Disabled      Full    Auto
xe-1/1/26   Enabled     Down    Disabled      Full    Auto
xe-1/1/27   Enabled     Down    Disabled      Full    Auto
xe-1/1/28   Enabled     Down    Disabled      Full    Auto
xe-1/1/29   Enabled     Down    Disabled      Full    Auto
xe-1/1/30   Enabled     Down    Disabled      Full    Auto
xe-1/1/31   Enabled     Down    Disabled      Full    Auto
xe-1/1/32   Enabled     Down    Disabled      Full    Auto
te-1/1/1(33)    Enabled     Up      Disabled      Full    10Gb/s
te-1/1/2(34)    Enabled     Up      Disabled      Full    10Gb/s
```

Forwarding Error Correction (FEC)

Introduction

Forwarding Error Correction (FEC) is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The sender sends the data together with a certain redundant error correction code. When the data is received at the receiver's end, it is checked according to the error correction code. If an error is found, the receiver recognizes it and corrects the error without data retransmission.

The FEC function can be applied to 100G, 40G and 25G ports of the switch and works only when all the three following conditions are matched:

- FEC function is enabled on both ends of the link.
- Optical modules are plugged in.
- Interface rate is auto or at the default value, i.g. 100G optical port works at 100Gb/s.

PICOS offers FEC algorithm RS-FEC (CL91) on 100G port and FEC BASE-R (CL74) on 40G port.

For 25G port, PICOS offers two different FEC algorithms on different switch platforms:

Trident 3, Maverick2, Helix5 and Tomahawk 2 platform switches support RS-FEC (CL108) mode, Tomahawk+/Tomahawk platform switches support BASE-R (CL74) mode.

> **NOTE：**
>
> - AS5812_54T and AS5812_54X don't support FEC.
> - The port can link up only when the FEC configurations and the FEC algorithm mode on both ends of the link are the same.
> - For 200G, 400G and 800G ports, the FEC function is enabled by default, and cannot be disabled.

Configuring FEC Function

Procedure

- Use the following command to enable or disable the FEC function on the 100G, 40G or 25G port of the switch.

  set interface gigabit-ethernet <*interface-name*> **fec** <**true | false**>

By default, FEC function is disabled on the 100G, 40G and 25G port of the switch.

Configuration Example

- Disable FEC function on the switch port xe-1/1/1.

```
admin@Xorplus# set interface gigabit-ethernet xe-1/1/1 fec false
admin@Xorplus# commit
```

- Enable FEC function on the switch port xe-1/1/2.

```
admin@Xorplus# set interface gigabit-ethernet xe-1/1/2 fec true
admin@Xorplus# commit
```

Verify the Configuration

- Use **run show interface gigabit-ethernet** *<interface-name>* command to view the interface status information of xe-1/1/2. Check the "**FEC Enable:** " field in the command output to find the FEC configuration.

```
admin@XorPlus# run show interface gigabit-ethernet xe-1/1/2
Physical interface: xe-1/1/2, Enabled, error-discard False, Physical link is Down
Interface index: 2, QSFP28 type: DAC, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full, FEC Enable: True
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Link fault signaling  ignore local fault:false, ignore remote fault:false
force up mode:false
Precision Time Protocol mode:none
Current address: a8:2b:b5:e0:88:c7, Hardware address: a8:2b:b5:e0:88:c7
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.....................0
  Output Packets....................0
  Input Octets......................0
  Output Octets.....................0
```

Configuring the Loopback Interface

The loopback interface is always Up to ensure network reliability.

The loopback interface has the following features:

- The loopback interface is always Up and has the loopback feature.
- The loopback interface can be configured with the mask of all 1s.

Based on the preceding features, the loopback interface has the following applications.

- The IP address of a loopback interface is specified as the source address of packets to improve network reliability.
- When no Router ID is configured for dynamic routing protocols, the maximum IP address of the loopback interface is configured as the router ID automatically.

The following commands can be used to configure a loopback interface：

set l3-interface loopback {**lo |** <*vrf-name*>} **address** <*ipv4-address*> **prefix-length 32**

set l3-interface loopback {**lo |** <*vrf-name*>} **address** <*ipv6-address*> **prefix-length 128**

The following command creates a IPv4 loopback interface in the default VRF.

```
admin@Xorplus# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@Xorplus# commit
```

The following commands can be used to disable a loopback interface.

```
admin@Xorplus# set l3-interface loopback lo2 disable true
admin@Xorplus# commit
```

The following commands can be used to bind the loopback interface to a VRF. Users can configure multiple loopback interfaces per VRF.

```
admin@Xorplus# set l3-interface loopback lo2 vrf vrf2
admin@Xorplus# commit
```

Layer 3 VLAN Interface Configuration

Configuring a Layer 3 VLAN Interface

The Layer 3 interface is a VLAN interface. Use the following configuration sequence:

1. Create a VLAN using the **set vlans vlan-id** command.
2. Associate an L3 interface with the VLAN using the **set vlans vlan-id l3-interface** command.
3. Configure the IP address and prefix length for the virtual interface using the **set l3-interface vlan-interface address prefix-length** command.

- When all the interfaces in a VLAN are link-down, the VLAN interface will be link-down. The VLAN interface will be link-up only when at least one of the member interfaces is link-up.
- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 192.168.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 192.168.2.1 prefix-length 24
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show l3-interface
vlan-2 Hwaddr C8:0A:A9:9E:14:9F, Vlan:2, State:DOWN
Inet addr: 192.168.1.1/24
fe80::ca0a:a9ff:fe9e:149f/64
Traffic statistics:
IPv4 Input Packets.....................0
IPv4 Forwarding Packets.....................0
IPv6 Input Packets.....................0
IPv6 Forwarding Packets.....................0
vlan-3 Hwaddr C8:0A:A9:9E:14:9F, Vlan:3, State:UP
Inet addr: 192.168.2.1/24
fe80::ca0a:a9ff:fe9e:149f/64
Traffic statistics:
IPv4 Input Packets.....................0
IPv4 Forwarding Packets.....................0
IPv6 Input Packets.....................0
IPv6 Forwarding Packets.....................0
admin@XorPlus#
```

Configuring the MTU

- When the MTU value is less than 1280 bytes, it will affect the normal functioning of IPv6. Therefore, set the MTU value of the VLAN interface to be greater than or equal to 1280 bytes for IPv6 to function normally.
- When modifying the MTU from a value less than 1280 bytes to a value greater than or equal to 1280 bytes, you need to restart the switch to resume the normal functioning of IPv6.

```
admin@Xorplus# set l3-interface vlan-interface vlan-2 mtu 2000
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring the Rate Limiting

L3 VLAN interface rate limit is applied to packets delivered out from the CPU, controlling shock of large flow on CPU, releasing the burden on CPU.

```
admin@Xorplus# set l3-interface vlan-interface vlan200 rate-limit 1024
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring 31-bit Prefixes IPv4 Address

PicOS supports configuring 31-bit prefixes on IPv4 point-to-point links. The point-to-point link has only two endpoints and broadcast support is not required. Two addresses in the subnet with 31-bit address prefix (the address with host ID all 0 and the address with host ID all 1) are allocated to the point-to-point hosts. For more details, refer to RFC 3021.

The following example commands configure the 31-bit prefixes IPv4 addresses 192.168.100.4 and 192.168.100.5 respectively on two switches for the point-to-point connected L3 interfaces.

```
#On Switch 1
admin@Switch1# set l3-interface vlan-interface vlan10 address 192.168.100.4 prefix-length 31
admin@Switch1# commit


#On Switch 2
admin@Switch2# set l3-interface vlan-interface vlan10 address 192.168.100.5 prefix-length 31
admin@Switch2# commit
```

Configuring Routed Interface

- Introduction of Routed Interface
- Configuration Notes of Routed Interface
- Configuring Routed Interface and Sub-interface
- Example for Configuring Routed Interface

Introduction of Routed Interface

- Routed Interface
- Reserved VLAN
- Sub-interface

Layer 3 interfaces, including VLAN interface, loopback interface, routed interface and sub- interface, share the same hardware resources. When configuring IP address, it is required that the IP address of different layer 3 interfaces in the same VRF cannot be in the same subnet. However, overlapped layer 3 interface addresses in different VRFs is supported.

> **NOTE:**
> To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Routed Interface

All Ethernet ports are layer 2 interfaces by default. When you need to use an Ethernet port for layer 3 communication, you can enable the Ethernet port as a routed interface. The routed interface is a layer 3 interface which can be assigned an IP address and can be configured with a routing protocol for connecting to other layer 3 routing devices.

A routed interface can be enabled on a physical port or a LAG interface. You can use the following commands to configure the routed interface:

set vlans reserved-vlan *<reserved-vlan>*

set interface gigabit-ethernet *<interface-name>* **routed-interface enable** <**true | false**>

set interface gigabit-ethernet *<interface-name>* **routed-interface name** *<string>*

set interface aggregate-ethernet *<lag-name>* **routed-interface enable <true | false>**

set interface aggregate-ethernet *<lag-name>* **routed-interface name** *<string>*

When enabling an Ethernet port/LAG interface as a layer 3 routed interface, a name for the routed interface should be configured by using the command **set interface gigabit-ethernet** *<interface-name>* **routed-interface name** *<string>*. This name will be referred to as the “interface name” in other CLI commands.

Reserved VLANs need to be configured on the device before configuring the routed interface.

Routed interface is mutually exclusive with the following layer 2 features, you have to delete all of the following configurations on the interface before enabling it as a routed interface, otherwise the routed interface commands will fail to commit.

set interface gigabit-ethernet *<interface-name>* **backup-port** *XX*
set interface aggregate-ethernet *<lag-name>* **backup-port** *XX*
set interface gigabit-ethernet *<interface-name>* **crossflow** *XX*
set interface aggregate-ethernet *<lag-name>* **crossflow** *XX*
set interface gigabit-ethernet *<interface-name>* **family** *XX*
set interface aggregate-ethernet *<lag-name>* **family** *XX*
set interface gigabit-ethernet *<interface-name>* **loopback true**
set interface gigabit-ethernet *<interface-name>* **port-security** *XX*
set interface aggregate-ethernet *<lag-name>* **port-security** *XX*
set interface gigabit-ethernet *<interface-name>* **static-ethernet-switching mac-address** *XX*
set interface aggregate-ethernet *<lag-name>* **static-ethernet-switching mac-address** *XX*
set interface gigabit-ethernet *<interface-name>* **voice-vlan** *XX*
set interface aggregate-ethernet *<lag-name>* **voice-vlan** *XX*
set protocols dhcp snooping trust-port *<trust-port>*
set protocols igmp-snooping vlan-id *<vlan-id>* **mrouter interface** *<interface-name>*
set protocols igmp-snooping vlan-id *<vlan-id>* **static group** *<group-address>* **interface** *<interface-name>*
set protocols dot1x interface *<interface-name>*
set interface gigabit-ethernet *<interface-name>* **breakout true**

Besides the layer 2 features listed above, routed interface does not support Spanning Tree Protocol (STP) and MAC learning. However, the Layer 2 feature of LLDP is supported on an Ethernet port enabled as routed interface.

As a layer 3 interface, routed interface supports layer 3 routing protocols, such as BGP/OSPF/static route/IGMP/PIM/BFD, and features such as VRRP/VRF/ARP/ IPv6 Neighbor Discovery/VXLAN/DHCP relay.

After a routed interface is enabled, you have to configure the following node to bring the routed interface up. Only after this, the corresponding sub-interfaces can be used normally.

set l3-interface routed-interface *<interface-name>*

Layer 3 sub-interfaces can be configured on the routed interface, so as to extend more layer 3 functions on the same physical port or LAG interface and conduct more flexible network topology design. Here, we call the routed interface the parent interface.

Reserved VLAN

The physical port/LAG interface that enabled routed interface is still consuming a special VLAN, although it is not allowed to explicitly configure VLANs for the routed interface by using the following commands:

set interface gigabit-ethernet *<interface-name>* **family ethernet-switching vlan members** *<vlan-id>*

set interface gigabit-ethernet *<interface-name>* **family ethernet-switching native-vlan-id** *<vlan-id>*

set interface aggregate-ethernet *<lag-name>* **family ethernet-switching vlan members** *<vlan-id>*

set interface aggregate-ethernet *<lag-name>* **family ethernet-switching native-vlan-id** *<vlan-id>*

Reserved VLANs need to be configured on the device with the command **set vlans reserved-vlan** *<reserved-vlan>* before configuring routed interface. Whenever a routed interface is configured, the system will automatically assign a VLAN internally to the routed interface from the reserved VLANs in order of smallest to largest.

The system supports up to 128 reserved VLANs.

VLAN 1 cannot be used as a reserved VLAN.

A reserved VLANs are VLANs dedicated to the routed interfaces (sub-interfaces are not included) and cannot be used for other interfaces, or other VLAN functions, such as PVLAN.

Reserved VLAN is mutually exclusive with the following settings, before configuring, please delete all these commands that uses the reserved VLAN, otherwise the reserved VLAN command will fail to commit.

set protocols dhcp snooping vlan *<vlan-id>*
set protocols igmp-snooping vlan-id *<vlan-id>*
set protocols dot1x block-vlan-id *<vlan-id>*
set protocols dot1x server-fail-vlan-id *<vlan-id>*
set vlans vlan-id *<vlan-id>* **private-vlan** *XX*

Note that: If you want to modify the value of the reserved VLANs, all the routed interface configurations need to be removed first.

You can use the commands **run show vlans** and **run show vlans routed-vlan** to check the VLAN information of all routed interfaces. For example,

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface name rif-te2
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set vlans reserved-vlan 80-85
admin@Xorplus# commit

admin@Xorplus# run show vlans
VlanID  Vlan Name           Tag        Interfaces
------  ------------------  --------   ------------------------------------------------------
1       default             untagged   te-1/1/1, xe-1/1/1, xe-1/1/2, xe-1/1/3, te-1/1/3
                                       xe-1/1/4, xe-1/1/5, te-1/1/5, xe-1/1/6, te-1/1/6
                                       te-1/1/7, te-1/1/8, te-1/1/9, te-1/1/10, te-1/1/11
                                       te-1/1/12, te-1/1/13, te-1/1/14, te-1/1/15, te-1/1/16
                                       te-1/1/17, te-1/1/18, te-1/1/19, te-1/1/20, te-1/1/21
                                       te-1/1/22, te-1/1/23, te-1/1/24, te-1/1/25, te-1/1/26
                                       te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30, te-1/1/31
                                       te-1/1/32, te-1/1/33, te-1/1/34, te-1/1/35, te-1/1/36
                                       te-1/1/37, te-1/1/38, te-1/1/39, te-1/1/40, te-1/1/41
                                       te-1/1/42, te-1/1/43, te-1/1/44, te-1/1/45, te-1/1/46
                                       te-1/1/47, te-1/1/48
                            tagged

80                          untagged   te-1/1/2
                            tagged

81                          untagged   te-1/1/4
                            tagged

82                          untagged
                            tagged

83                          untagged
                            tagged

84                          untagged
                            tagged

85                          untagged
                            tagged

admin@Xorplus# run show vlans routed-vlan
VlanID  Vlan Name           Tag         Interfaces     Routed-interfaces
------  ------------------  --------    ------------   --------------------
80                          untagged    te-1/1/2        rif-te2
81                          untagged    te-1/1/4        rif-te4
```

NOTE:

- When using the command **set interface gigabit-ethernet** *<interface-name>* **disable true** to disable the physical port, it will also bring down the associated routed interface.
- The member port of a LAG port cannot be enabled as a routed interface, correspondingly, the physical port enabled as a routed interface cannot be configured as a LAG member port.
- To perform layer 3 forwarding, don't forget to configure the command **set ip routing enable true** to enable IP routing.

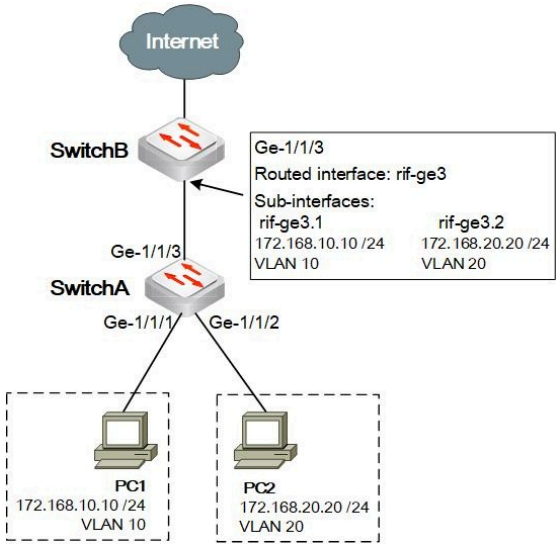
Sub-interface

A layer 3 sub-interface is a virtual interface configured under a physical port or LAG interface, which has been enabled as a routed interface. The routed interface is called the parent interface. Sub-interface is a layer 3 interface, and you can configure IP address for it. This enables routing and communication between multiple VLANs configured under a single physical interface by dividing it into multiple sub-interfaces.

The sub-interface name is a string of up to 15 alphanumeric characters (including three special characters . – and @). The suggested naming convention for the sub-interfaces should be like this: parent name (for example, rif-ge2) followed by a period and then by a number that is unique to that sub-interface, for example, rif-ge2.1, rif-ge2.2 and so on.

As shown in the figure below, when a layer 3 device Switch B connects to a layer 2 network device Switch A through a routed interface. The ports of the Switch A are divided into different VLANs, in order for the layer 3 routed interface on Switch B to correctly identify different VLAN messages, it is necessary to create multiple sub-interfaces on the routed interface to correspond to the VLANs of downstream devices respectively. This ensures that users in different VLANs can communicate normally. We provide a detailed configuration process about this example in section Example for Configuring Routed Interface.

Figure 1. Routed Interface and Sub-interface Application



When creating a sub-interface, VLAN ID needs to be specified at the same time. Different sub-interfaces of the same parent interface cannot be configured to the same VLAN.

Different layer 3 interfaces belong to different subnets, and the sub-interfaces of different parent interfaces can be configured with the same VLAN. But even if they are in the same VLAN, the two sub-interfaces are in different flood domains.

When configuring the routed interface, you have to run the following command to bring up the parent routed interface. Only after this, the corresponding sub-interfaces can be used normally.

set l3-interface routed-interface <*interface-name*>

If the parent interface is down, then all of its sub-interfaces will also be down. When using the command **set interface gigabit-ethernet** <*interface-name*> **disable true** to disable the physical port, it will also bring down the associated routed interface and its sub-interfaces.

When sub-interfaces are used for inter-VLAN routing, the data flow will occupy the bandwidth of the entire physical interface. This can lead to communication bottlenecks when the network is busy. To balance the traffic load on the physical interface, it is recommended that the sub-interfaces be configured on multiple physical interfaces.

Pay attention to the following precautions before configuring the sub-interfaces:

- Enable the Ethernet port as a routed interface before configuring the sub-interfaces.
- Define the VLAN ID by using the command **set vlans vlan-id** <*vlan-id*> before configuring the sub-interface and adding to VLAN.
- The IP address for each sub-interface should be in a different subnet from all the other sub-interfaces under that parent interface. That is, the IP subnets of all the sub-interfaces should be unique under the same parent interface.
- It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.
- On greyhound2 switches (including Dell N22xx series switches and N3208PX-ON), the sub-interface does not support user defined VRF and can only be used in the default VRF.
- The sub-interface of LAG port does not support user defined VRF and can only be used in the default VRF.

Configuration Notes of Routed Interface

Pay attention to the following precautions before configuring the routed interfaces:

- To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.
- Routed interface and sub-interface are supported in VXLAN underlay configuration, but not in VXLAN overlay configuration. In VXLAN underlay configuration, if the outgoing interface of a VXLAN tunnel is a sub-interface, then the VLAN of this sub-interface is not allowed to be assigned to other interfaces.
- If a VLAN has already been configured in other layer 3 functions, such as been assigned to a sub-interface, then it cannot be used for layer 2 functions, for example, it cannot be assigned to other interfaces, or be used in other layer 2 functions, such as PVLAN.

Configuring Routed Interface and Sub-interface

- Configuring Routed Interface
- Configuring Sub-interface
- (Optional) Other Settings for Routed Interface and Sub-interface
- Checking the Configuration

Configuring Routed Interface

Step 1 Configure reserved VLAN for the use of routed interface.

set vlans reserved-vlan <*reserved-vlan*>

Step 2 Enable Ethernet port as a layer 3 routed interface.

set interface gigabit-ethernet <*interface-name*> **routed-interface enable <true | false>**

set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

Step 3 Run the following command to bring up the parent routed interface. Only after this, the corresponding sub-interfaces can be used normally.

set l3-interface routed-interface <*interface-name*>

Step 4 Enable IP routing to perform layer 3 forwarding.

set ip routing enable true

Step 5 Commit the configuration.

commit

Configuring Sub-interface

Step 1 Configure the VLAN.

set vlans vlan-id <*vlan-id*>

Step 2 Create sub-interface and configure its IP address.

set interface gigabit-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

set l3-interface routed-interface <*interface-name*> address <*ip-address*> prefix-length <*prefix-number*>

Step 3 Commit the configuration.

commit

(Optional) Other Settings for Routed Interface and Sub-interface

Step 1 Configure the CPU egress rate limit for the routed interfaces and sub-interfaces.

set l3-interface routed-interface <*interface-name*> **rate-limit** <*rate-limit*>

Step 2 Configure the MTU for the routed interfaces. It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.

set l3-interface routed-interface <*interface-name*> **mtu** <*mtu-value*>

Step 3 Bind the routed interface and sub-interface to the VRF.

set l3-interface routed-interface <*interface-name*> **vrf** <*vrf-name*>

Step 4 Commit the configuration.

commit

Checking the Configuration

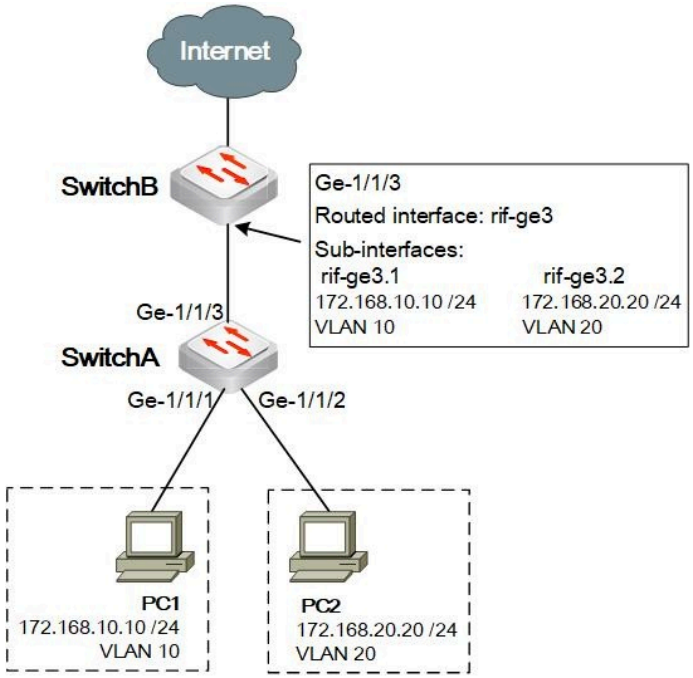
- Run the command **run show vlans routed-vlan** to check the VLAN information of the routed interfaces and sub-interfaces.
- Run the command **run show interface routed-interface brief** to check the brief interface information of the routed interfaces and sub-interfaces.
- Run the command **run show l3-interface routed-interface** <*interface-name*> to check the detailed layer 3 interface information of a specific routed interface or sub-interface.

Example for Configuring Routed Interface

- Networking Requirements
- Procedure
  - Switch A
  - Switch B

Networking Requirements

Figure 1. Routed Interface and Sub-interface Configuration Example



As shown in Figure 1, PC1 and PC2 are local computers which belong to VLAN 10 and VLAN 20 respectively, and they are in different network segments 172.168.10.10/24 and 172.168.20.20/24 respectively. They connect to the layer 3 device Switch B through the layer 2 device Switch A. There is only one free physical port ge-1/1/3 on Switch B. In this scenario, it is required that Switch B can connect to two different network segments through only one physical port.

This can be accomplished by enabling interface ge-1/1/3 as a routed interface, under it configuring two different sub-interfaces to connect to PC1 and PC2 respectively.

Complete the following configurations on the Switch B:

- Enable interface ge-1/1/3 as a routed interface and name its layer 3 interface as rif-ge3.
- Create two layer 3 sub-interfaces, rif-ge3.1 and rif-ge3.2, assign IP addresses 172.168.10.10/24 and 172.168.20.20/24, to serve as gateway addresses for VLAN 10 and VLAN 20 users, respectively.

Procedure

Switch A

As a layer 2 switch, Switch A needs to configure VLANs and add the access ports to the corresponding VLANs.

```
admin@XorPlus# set vlans vlan-id 10
admin@XorPlus# set vlans vlan-id 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 20
admin@XorPlus# commit
```

Switch B

Step 1 Configure two VLANs.

```
admin@XorPlus# set vlans vlan-id 10
```

```
admin@XorPlus# set vlans vlan-id 20
```

Step 2 Configure reserved VLAN for the use of routed interface.

```
admin@XorPlus# set vlans reserved-vlan 80-90
```

Step 3 Enable Ethernet port ge-1/1/3 as a layer 3 routed interface.

> **NOTE:**
> To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 routed-interface enable true
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 routed-interface name rif-ge3
```

Step 4 Run the following command to bring up the parent routed interface. Only after this, the corresponding sub-interfaces can be used normally.

```
admin@XorPlus# set l3-interface routed-interface rif-ge3
```

Step 5 Create the sub-interfaces and specify the IP addresses.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 routed-interface sub-interface rif-ge3.1 vlan-id 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 routed-interface sub-interface rif-ge3.2 vlan-id 20
admin@XorPlus# set l3-interface routed-interface rif-ge3.1 address 172.168.10.10 prefix-length 24
admin@XorPlus# set l3-interface routed-interface rif-ge3.2 address 172.168.20.20 prefix-length 24
```

Step 6 Enable IP routing to perform layer 3 forwarding.

```
admin@XorPlus# set ip routing enable true
```

Step 7 Commit the configuration.

```
admin@XorPlus# commit
```

Step 8 Verify the configuration.

- After the above configurations are completed, ping PC1 from PC2 to test the connectivity.
- Run the command **run show vlans routed-vlan** to check the VLAN information of the routed interfaces and sub-interfaces.

```
admin@SwitchB# run show vlans routed-vlan
VlanID  Vlan Name           Tag        Interfaces     Routed-interfaces
------  ------------------  --------   ------------   --------------------
10      default             tagged      ge-1/1/3       rif-ge3.1
20      default             tagged      ge-1/1/3       rif-ge3.2
80                          untagged      ge-1/1/3       rif-ge3
```

- Run the command **run show interface routed-interface brief** to check the brief information of the routed interfaces and sub-interfaces.

```
admin@Xorplus# run show interface routed-interface brief
Interface       RoutedIfName     SubRoutedIfName  VLANID  Management  Status  Flow Control   Duplex  Speed    Descr
--------------  ---------------  ---------------   ------ ----------  ------  ------------   ------  -------  -----
ge-1/1/3        rif-ge3                           80      Enabled     Up      Disabled       Full     Auto
                                 rif-ge3.1         10
                                 rif-ge3.2         20
```

- Run the command **run show l3-interface routed-interface** <*interface-name*> to check the detailed layer 3 information of a specific routed interface or sub-interface.

```
admin@Xorplus# run show l3-interface routed-interface rif-ge3
rif-ge3         Hwaddr 18:5A:58:1F:63:A1, Vlan:80, MTU: 1500, State:UP
            Inet addr: 120:1:1::49/64
                       fe80::1a5a:5820:131f:63a1/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.............................0
              IPv4 Forwarding Packets........................0
              IPv6 Input Packets.............................0
```

```
        IPv6 Forwarding Packets.....................0
```

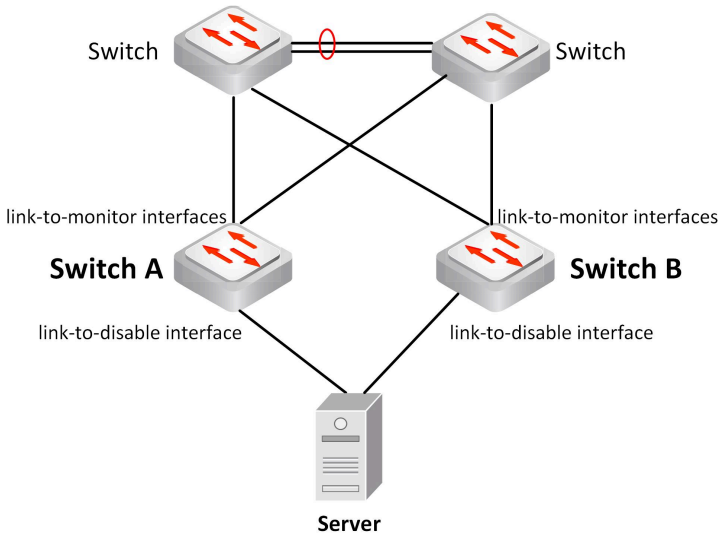
Uplink Failure Detection

- Description
- Configuring Uplink Failure Detection
- Uplink Failure Detection Configuration Example
  - Networking Requirements
  - Procedure
    - Switch A
    - Switch B

Description

Uplink Failure Detection (UFD) provides a mechanism to disable all the associated downlink interfaces when all the uplink interfaces go down, which is very useful in the case of network redundancy for the downlink server going with network adapter teaming.

Figure 1. Uplink Failure Detection



All the network interface cards (NICs) in a network adapter teaming works under stand-by mode with the same IP address. Namely, when the primary link goes down, the server automatically changes to the secondary link. If uplink failure detection is enabled, the switch monitors the uplink interfaces (link-to-monitor interfaces). When all the uplink interfaces go down, the switch will disable all the associated downlink interfaces (link-to-disable interface). When the server detects disabled downlink interfaces on the switch side, it switches over to the secondary link, which helps to quickly detect link failures and reduce network packet loss.

Configuring Uplink Failure Detection

NOTEs:

- Only the physical interfaces or LAG interfaces can be configured as UFD uplink interfaces or downlink interfaces, logical interfaces are not supported.
- In the same UFD group, the same interface cannot be configured as both the UFD uplink interface and the downlink interface.
- The same interface can be configured as the UFD downlink interface only in one UFD group. That is, it is not allowed to configure the same interface as the UFD downlink interface in different UFD groups.

Step 1 Configure the uplink interface to an uplink failure detection group. Repeat this step to add more uplink interfaces to the uplink failure detection group.

set interface ufd <*ufd-group-name*> **link-to-monitor** <*interface-name*>

Step 2 Configure the downlink interface to an uplink failure detection group. Repeat this step to add more downlink interfaces to the uplink failure detection group.

set interface ufd <*ufd-group-name*> **link-to-disable** <*interface-name*>

Step 3 Commit the configurations.

commit

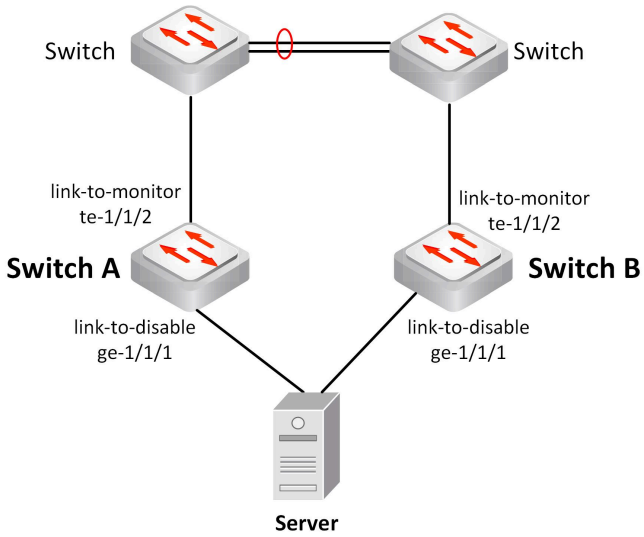
Step 4 View the uplink failure detection configuration information and status.

run show interface ufd

Uplink Failure Detection Configuration Example

Networking Requirements

Figure 2. Uplink Failure Detection Configuration Example



As shown in **Figure 2**, on the Server, all the network interface cards (NICs) in a network adapter teaming works under stand-by mode with the same IP address. Namely, when the primary link goes down, the server automatically changes to the secondary link.

To quickly detect link failures and reduce network packet loss, uplink failure detection can be enabled on Switch A and Switch B separately to monitor the uplink interfaces (link-to-monitor interfaces) on each side. When all the uplink interfaces on one switch side go down, Switch A/Switch B will disable all the associated downlink interfaces (link-to-disable interface). When the server detects disabled downlink interfaces on one switch side, it switches over to the secondary link. For simplicity, there is only one uplink interface and one downlink interface in each UFD group in this configuration example.

This example does not describe how to configure the dual-homed server or the aggregation switches. Please refer to the documentation for each of these devices for more information.

Procedure

Switch A

Step 1 Configure the uplink interface to an uplink failure detection group.

```
admin@SwitchA# set interface ufd ufd1 link-to-monitor te-1/1/2
```

Step 2 Configure the downlink interface to an uplink failure detection group.

```
admin@SwitchA# set interface ufd ufd1 link-to-disable ge-1/1/1
```

Step 3 Commit the configurations.

```
admin@SwitchA# commit
```

Step 4 View the uplink failure detection configuration information and status. Hence the uplink interface and the downlink interface are up, so in the result the status of *Failure Action* is **Inactive**.

```
admin@SwitchA# run show interface ufd
UFD: ufd1
------------------------------------------------------
Uplink        : te-1/1/2
Downlink      : ge-1/1/1
Failure Action: Inactive
```

Switch B

Step 1 Configure the uplink interface to an uplink failure detection group.

```
admin@SwitchB# set interface ufd ufd1 link-to-monitor te-1/1/2
```

Step 2 Configure the downlink interface to an uplink failure detection group.

```
admin@SwitchB# set interface ufd ufd1 link-to-disable ge-1/1/1
```

Step 3 Commit the configurations.

```
admin@SwitchB# commit
```

Step 4 View the uplink failure detection configuration information and status. Hence the uplink interface and the downlink interface are up, so in the result the status of *Failure Action* is **Inactive**.

```
admin@SwitchB# run show interface ufd
UFD: ufd1
------------------------------------------------------
Uplink        : te-1/1/2
Downlink      : ge-1/1/1
Failure Action: Inactive
```

Layer 2 Switching Configuration

This chapter describes the configuration steps of Layer 2 switching, including MAC address learning, LLDP, LACP, 802.1Q VLAN, flow control, mirroring, storm control, and the Spanning Tree Protocol (STP/RSTP/MSTP).

- Static MAC entries and Dynamic MAC Address Learning
- Cut-Through Switching Method
- MLAG Configuration
  - Principle of MLAG
  - Configuration Notes and Constraints
  - Configuring MLAG
  - Configuration Example of MLAG
    - Example for Configuring a Basic MLAG
    - Example for Configuring MLAG with Active-Active-VRRP
    - Example for Configuring MLAG with DHCP Relay
    - Example for Configuring MLAG with DHCP Snooping
    - Example for Configuring MLAG with IGMP Snooping
    - Example for Configuring MLAG with Rapid PVST+
    - Example for Configuring MLAG with VXLAN
  - MLAG Maintenance and Troubleshooting
    - How to bind a LAG interface to the MLAG link?
    - How to check whether the VLAN configuration on the two peer-link ports are consistent?
    - How to confirm whether the MAC address table has been correctly synchronized?
    - How to enable MLAG traceoptions
    - How to ensure the reliability of the peer link?
    - How to verify configurations on MLAG peer are consistent?
    - How to verify MLAG link status?
    - How to verify MLAG neighbor status?
    - How to verify that the peer link connection status is normal?
    - How to view and clear MLAG statistics?
- VLAN Configuration
  - Configuring MAC-based VLAN
  - MAC Trace
  - Configuring Port-based VLAN
- GVRP
  - Overview of GVRP
  - Configuring GVRP
  - Example for Configuring GVRP
- MVRP
  - Overview of MVRP
  - Configuring MVRP
  - Example for Configuring MVRP
- Q-in-Q Basic Port Configuration
- Private VLAN Configuration Guide
  - Introduction of PVLAN
  - Configuration Notes of PVLAN
  - Configuring PVLAN
  - Example for Configuring PVLAN
  - Example for Configuring DHCP Snooping with PVLAN
- Voice VLAN Configuration Guide
  - Principle of Voice VLAN
  - Configuration Notes of Voice VLAN
  - Configuring Voice VLAN
  - Configuration Example of Voice VLAN
- Link Aggregation Configuration
  - Static Link Aggregation (LAG) Configuration
  - Link Aggregation Control Protocol (LACP) Configuration
  - LAG Hashing Configuration
    - LAG Hashing Configuration and Example
    - LAG Hash Mapping
    - Resilient LAG Hashing Configuration and Example
  - LACP Fallback
  - Configuring LACP Fast Rate
  - LAG Specification of Different Platforms
- Symmetric Hash for LAG Configuration Example
- LLDP Configuration (Link Layer Discovery Protocol)
- LLDP MED Configuration
- MSTP Configuration

- MSTP Configuration Example
- Rapid PVST+ Configuration
- Rapid PVST+ Configuration Example
- BPDU Tunneling Configuration
- UDLD Configuration
- LFS Configuration
- Storm Control in Ethernet Port Configuration
- Ethernet Ring Protection Switching (ERPS)
  - Overview of ERPS
  - Configuration Notes and Constraints of ERPS
  - Configuring ERPS
  - Example for Configuring ERPS (Single Ring)
  - Example for Configuring ERPS (Intersection Rings)
- Loopback Detection
  - Overview of Loopback Detection
  - Configuring Loopback Detection

Static MAC entries and Dynamic MAC Address Learning

You can configure a static MAC entry in the FDB and manage dynamic MAC address learning (for example, configuring aging time or deleting the dynamic MAC address entry).

Configuring a Static MAC Entry and Managing the FDB

```
admin@PICOS# set interface gigabit-ethernet ge-1/1/1 static-ethernet-switching mac-address 22:22:22:22:22:22 vlan 1
admin@PICOS# set interface ethernet-switching-options mac-table-aging-time 60
admin@PICOS# commit
Commit OK.
Save done.
admin@PICOS# run show ethernet-switching table
Total entries in switching table: 0
Static entries in switching table: 0
Dynamic entries in switching table: 0

VLAN MAC address Type Age Interfaces User
---- ----------------- --------- ---- ---------------- ----------
admin@PICOS# run clear ethernet-switching table ge-1/1/1
admin@PICOS# run show ethernet-switching table
Total entries in switching table: 0
Static entries in switching table: 0
Dynamic entries in switching table: 0
VLAN MAC address Type Age Interfaces User
---- ----------------- --------- ---- ---------------- ----------

admin@PICOS#
```

Cut-Through Switching Method

By default, the switch forwards the packets in a cut-through switching method. That is, the switch begins forwarding a packet before the entire frame is received, normally as soon as the destination address is processed. This process reduces latency. Error handling is performed by the destination devices. User can configure the switch to the "store-and-forward" method with the commands below.

> P-3290, P-3295, P-3297 and 4610 series switches don't support cut-through mode.

Configuring your Switch to the Store-and-Forward Method

```
admin@XorPlus# set interface cut_through_mode false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

MLAG Configuration

- Principle of MLAG
- Configuration Notes and Constraints
- Configuring MLAG
- Configuration Example of MLAG
  - Example for Configuring a Basic MLAG
  - Example for Configuring MLAG with Active-Active-VRRP
  - Example for Configuring MLAG with DHCP Relay
  - Example for Configuring MLAG with DHCP Snooping
  - Example for Configuring MLAG with IGMP Snooping
  - Example for Configuring MLAG with Rapid PVST+
  - Example for Configuring MLAG with VXLAN
- MLAG Maintenance and Troubleshooting
  - How to bind a LAG interface to the MLAG link?
  - How to check whether the VLAN configuration on the two peer-link ports are consistent?
  - How to confirm whether the MAC address table has been correctly synchronized?
  - How to enable MLAG traceoptions
  - How to ensure the reliability of the peer link?
  - How to verify configurations on MLAG peer are consistent?
  - How to verify MLAG link status?
  - How to verify MLAG neighbor status?
  - How to verify that the peer link connection status is normal?
  - How to view and clear MLAG statistics?

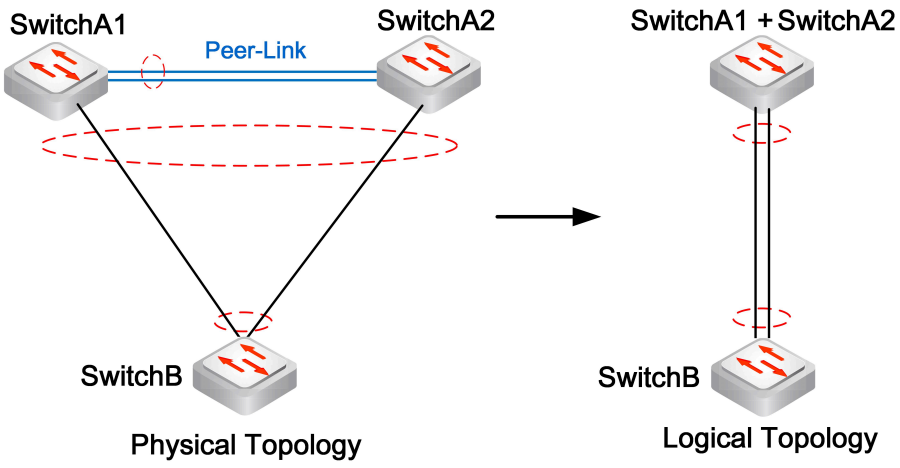
Principle of MLAG

- Definition
- Basic Concepts
- MLAG State Machine
  - MLAG Neighbor State
  - MLAG Interface State
- MLAG Control Plane Messages
- MAC Synchronization
- Configuration Consistency Check
  - Type 1 Configuration Consistency Parameters
  - Type 2 Configuration Consistency Parameters
  - Type 3 Configuration Consistency Parameters
  - Type 4 Configuration Consistency Parameters
  - Type 5 Configuration Consistency Parameters
  - Type 6 Configuration Consistency Parameters
- Single-homed Port
- Flood Control
- MLAG Peer-Gateway
- Multi-layer MLAG Application Networking
- Interoperability with Other Features
  - LACP
  - Rapid PVST+
  - DHCP Snooping & DHCP Relay
  - IGMP Snooping
  - VXLAN
  - ARP Inspection
- Traffic Forwarding in Typical Fault Scenarios
  - Downstream Link from Access Switch Down
  - Upstream Link to Layer-3 Device Down
  - MLAG Node Fault
  - MLAG Peer-link Down
- Backward Compatibility

Definition

MLAG (Multi-chassis Link Aggregation Group) as the name suggests, deploys LAG (Link Aggregation Group) technology to different member ports on a pair of devices which appear to be on a single device to the downstream third device in Layer 2. The figure below shows the physical topology and the logical topology of the MLAG network in Layer 2. The two MLAG peer devices, SwitchA1 and SwitchA2, maintain communication by exchanging MLAG control plane messages and MAC address learning of the LAG interface to ensure MAC synchronization using L2 multicast packets. The downstream device could be any endpoint equipment (L2 switch or server) that supports LACP Link Aggregation technology. It won't get a feel that there are two devices linked with it at the other end of the link when dual-homing to the network through the MLAG peer devices.

Figure 1. Physical Topology and Logical Topology of the MLAG Networking



MLAG is mainly applied in scenarios where a downstream switch or host has to or needs to dual-access to the network. In **Figure 1**, before deploying MLAG, suppose SwitchB single-accesses to the network through SwitchA1 when spanning tree is enabled. If SwitchA1 device fails or the link fails, SwitchB fails to communicate with the network. By using MLAG, the downstream switch or host can dual-access to the network through SwitchA1 and SwitchA2 which enables link-level and device-level redundancy and protection.

This provides redundancy by giving the downstream switch or host two uplink paths as well as full bandwidth utilization since the MLAG domain appears to be a single switch to Spanning Tree Protocol (STP). So, there are no blocked ports as the MLAG domain appears to STP as a single switch.

As MLAG has the following advantages, it can be used to build a highly resilient and highly reliable Layer 2 network.

- Increased Bandwidth

MLAG aggregates multiple Ethernet ports across two switches, this increases the uplink bandwidth. The maximum bandwidth of the link aggregation interface can reach the sum of the bandwidths of individual MLAG member ports.

- Higher Reliability

Dual-working mechanism to ensure high reliability. When a link or device fails, traffic can be switched to the other available member links or device to improve the reliability of the MLAG domain.

- Load Balancing

  In an MLAG domain, you can achieve load balancing on each active aggregation interface link.

Basic Concepts

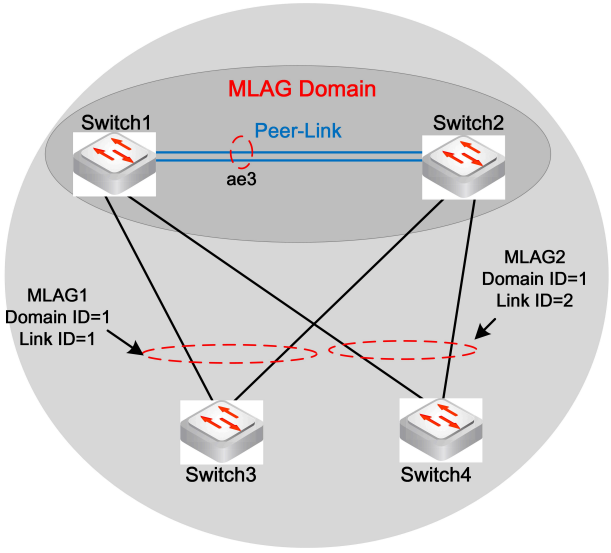
- **MLAG domain and domain ID**

MLAG domain defines the topology range of the MLAG calculations and control. An MLAG domain includes a pair of MLAG peer switches, the MLAG peer-link and the MLAG member ports. The MLAG domain ID is a unique identifier for an MLAG domain, which should be configured identically on each MLAG peer device in the same MLAG domain.

Currently, only one MLAG domain is allowed to be configured on one MLAG device. A pair of MLAG peer devices can be connected to different third-party devices to form different MLAGs. An MLAG domain can hold multiple MLAGs.

Figure 2 shows an MLAG domain with multiple MLAGs, where Switch1, Switch2 and the MLAG member ports connected to Switch3 form an MLAG1; Switch1, Switch2 and the MLAG member ports connected to Switch4 form another MLAG2.

Figure 2. Multiple MLAGs Network



Use the **run show mlag domain** command to view the MLAG domain information:

```
admin@Xorplus# run show mlag domain summary

Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 0
-------------------------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status    Config Matched       MAC Synced  # of Links
---------  ---------------  ---------  ---------------    --------------      ----------  ----------
ae23       1.1.1.2          4088        ESTABLISHED         Yes                Yes          2
```

NOTE:

- MLAG domain ID is required to be unique within the Layer 2 network.
- The maximum number of MLAG interfaces/ports supported by the system is subject to the maximum number of LAGs supported by the switch. The maximum number of LAGs supported by each model is described in the command reference **set interface aggregate-ethernet** <*lag_name*>, the link is Collection of Feature Specification of Different Platforms.

- **MLAG domain MAC**

Each MLAG domain has a unique domain ID which should be different between different MLAG domains. Once configured, both MLAG peer devices use the MLAG domain ID to automatically produce a unique MLAG domain MAC address which is defined as **48:6E:73:FF:00:**<***MLAG domain ID in hexadecimal***>. For example, if the MLAG domain ID is 12, then the corresponding MLAG domain MAC address would be 48:6E:73:FF:00:0C.

MLAG domain MAC address is identical on both MLAG peer devices, it is used by LACP as part of system ID and by STP as part of bridge ID to communicate with other L2 devices. Use the command **run show mlag domain** {<*domain-id*>| **summary**} to show the MLAG domain information which includes the MLAG domain MAC.

- **MLAG peer**

MLAG peer devices are a pair of switches that enables the MLAG function, which are defined as MLAG **Node 0** or **Node 1**. Users have to use the CLI command **set protocols mlag domain** <*domain-id*> **node** <**0 | 1**> to specify the Node ID for the MLAG peer devices. If one of the MLAG peer devices is configured as Node 0, the other one should be configured as Node 1. The two nodes are all active, providing a reliable dual-access to the network for the MLAG access device.

The two nodes function equally and are not distinguished as master or slave. In most application scenarios, the two nodes have no difference, except for the following two cases:

1. The single-homed port uses the original port ID on Node 0 peer device, however, an offset **1024** is added to the **Port Index** as a new port ID on Node 1.
2. The MLAG member ports use the original port ID on Node 0 peer device, however, an offset **512** is added to the **Link ID** as a new port ID on Node 1.

We can see the port ID information in the display of LACP/STP related show command and BPDU packets.

- **MLAG peer link**

MLAG peer link is the direct link between MLAG peer devices, used for transmitting part of the data traffic, MLAG state and MLAG control plane messages. Use the **set protocols mlag domain** <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-link** <*peer-interface-name*> command to configure the remote peer-link port IP and the local peer-link interface. The interfaces directly connected to the two ends of the peer-link are peer-link ports.

A specified VLAN MUST be assigned to the peer-link interface, MLAG peer VLAN, which is dedicated to transmitting MLAG control plane messages and not transmitting data messages. Peer VLAN is always set to forwarding in order to allow MLAG information negotiation between MLAG peers. The following CLI commands is used to configure MLAG peer VLAN, the recommended value is 4088.

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-vlan** <*vlan-id*>

If peer-link is down for any reason, MLAG control plane messages cannot be exchanged properly, causing the MLAG system to operate abnormally. Especially when peer-link is down, but both the MLAG member ports are up, the split-brain failure scenario occurs. The system cannot be automatically recovered in this scenario.

Therefore, to ensure the reliability of peer-link, note the following points when configuring and deploying peer link:

1. Only one peer link connecting the two peer devices is allowed in an MLAG domain.
2. When configuring the peer link, only one LAG port can be used as peer link.
3. Use a LAG port with at least two **directly connected** physical ports to guarantees reliable communication between the peer devices on the peer link. Use of any intermediate transmission device between the two peer devices on the peer link is not allowed. All of the directly connected physical ports should be added into one LAG port to form the peer-link. We don't support more than one L2 connection between MLAG peer switches.
4. 10G or 40G speed ports should be used for peer link to enough bandwidth is provided when the network is deployed.
5. Any manual action to shut down the peer link is strictly forbidden.
6. Any MLAG VLAN and non-MLAG VLAN traffic MUST be allowed on MLAG peer-link.
7. When numerous rapid PVST+ instances are configured, exceeding the default BPDU queue processing rate in CPU will result in BPDU packets loss or network loops. To resolve this problem, you can use the following CoPP command to increase the maximum bandwidth of BPDU queue. The default value is 80pps.

   set class-of-service scheduler bpdu-scheduler max-bandwidth-pps <*value*>

8. When numerous MLAG instances are configured, exceeding the default MLAG queue processing rate in CPU will result in MLAG control packets loss. To resolve this problem, you can use the following CoPP command to increase the maximum bandwidth for MLAG and MLAG MAC SYNC queues. The default value is 80pps.

   set class-of-service scheduler mlag-scheduler max-bandwidth-pps <*value*>

   set class-of-service scheduler mlag-mac-sync-scheduler max-bandwidth-pps <*value*>

NOTE:

- When spanning tree protocol is enabled, the peer link port is always in forwarding state and won't participate in the spanning tree calculation after peer link is established.
- It is strongly recommended to use LACP protocol when configuring the peer link port.

- **MLAG member port**

MLAG member port is the LAG port on the MLAG peer devices that interconnects to the downstream device.

Usually, we configure MLAG member ports on the MLAG peer devices with the same LAG ID to form an MLAG. However, this is not required.

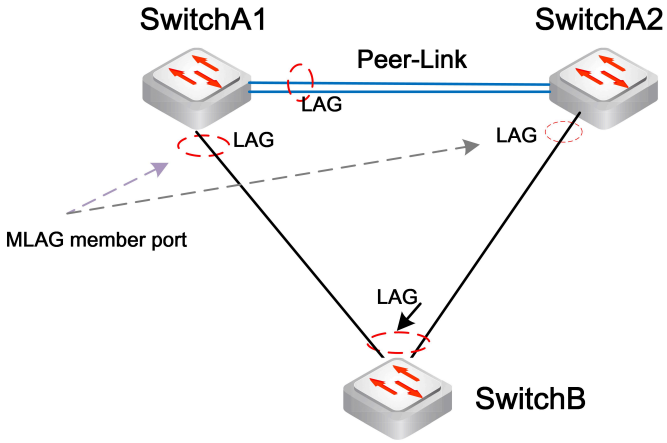
We have to bind the MLAG member port to the MLAG link ID. The paired MLAG member ports of the same MLAG must be bound to the same MLAG link ID. Different MLAGs are identified by different link IDs. For example we have two MLAGs in an MLAG Domain then link ID 1 could be used to identify one MLAG while link ID 2 could be used to identify the other MLAG in the MLAG Domain.

After all the MLAG configurations are finished, MLAG peer devices send MLAG control plane messages to each other to determine an MLAG pair. Upon receiving the MLAG Control message from the peer device, the local device determines whether the link ID carried in the MLAG Control message is the same as that of the local. If the link IDs configured on the two devices are the same, the two devices make an MLAG pair successfully.

User can use command **run show mlag link** to show the information about each MLAG and the MLAG member ports status.

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

Figure 3. MLAG Member Port



When accessing the MLAG domain, the access devices are required to support LAG protocol. As shown in Figure 3, SwitchB is required to configure a LAG interface to interconnect to the MLAG member ports.

NOTE:

It is strongly recommended to use LACP protocol when configuring the LAG interface.

MLAG State Machine

The MLAG state machine describes the state of the MLAG peer link and the MLAG member ports on the local device and the remote peer device. The MLAG state machine facilitate link fault detection and recovery. The system defines MLAG neighbor state and MLAG interface state to establish peer link and different MLAGs configured in this MLAG Domain.

MLAG uses the TCP protocol for reliably transmitting the MLAG control messages between the two peer devices to exchange the MLAG state change. The system changes the state based on the local MLAG state and the received peer MLAG Control message. You can view the MLAG interface state, and MLAG neighbor state by using related show commands.

MLAG Neighbor State

MLAG neighbor state shows the global status of MLAG peer device and peer-link, including the following values:

- **IDLE**: The initial state of the global neighbor state machine when MLAG peer-link is configured.
- **CONNECTING**: The peer-link ports are up. The peer-link connection is started. Both MLAG peers try to setup a TCP connection to each other.
- **ESTABLISHED**: This state indicates that peer-link connection between the MLAG peer devices is established, the peer session and neighbor relationship is setup.

You can use the **run show mlag domain** {*<domain-id>*|**summary**} command to view the MLAG peer-link configuration information and the neighbor state. For example,

```
admin@Xorplus# run show mlag domain summary
Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 0
-------------------------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status    Config Matched       MAC Synced  # of Links
---------  ---------------  ---------  ---------------    --------------      ----------  ----------
ae23       1.1.1.2          4088        ESTABLISHED         Yes                Yes          2
```

MLAG Interface State

MLAG interface state defines the status of peer link and MLAG member port, including the following values:

- **INIT**: The initial state of MLAG, MLAG is disabled and no information is exchanged in this state.
- **IDLE**: In this state, peer-link is configured, MLAG peer device initiates a TCP connection with the peer and changes its state. However, the peer-link session has not been established, MLAG link state switches from INIT to IDLE.
- **DOWN**: In this state, peer-link session is established, that is, the MLAG neighbor state is ESTABLISHED, but the MLAG member port is not configured on the MLAG peer device. If the local MLAG member port is down, then the MLAG interface state is DOWN.
- **STANDBY**: In this state, peer-link session is established, that is, the MLAG neighbor state is ESTABLISHED, but the MLAG member port is not configured on the MLAG peer device. If the local MLAG member port is up, then the MLAG interface state is STANDBY.
- **AS_DOWN**: In this state, peer-link session is established, that is, the MLAG neighbor state is ESTABLISHED. MLAG member ports are configured on both MLAG devices. If the MLAG member ports on both sides are down, the MLAG interface state is AS_DOWN.
- **AS_PEER:** In this state, peer-link session is established, that is, the MLAG neighbor state is ESTABLISHED. MLAG member ports are configured on both MLAG devices. If the local MLAG member port is down but peer MLAG member port is up, then the MLAG interface state is AS_PEER.
- **AS_LOCAL:** In this state, peer-link session is established, that is, the MLAG neighbor state is ESTABLISHED. MLAG member ports are configured on both MLAG devices. If the local MLAG member port is up but peer MLAG member port is down, then the MLAG interface state is AS_LOCAL.
- **FULL:** Peer session is established and MLAG member ports on both peer devices are up.

In brief, it can be summarized as the following table:

MLAG Interface State	Peer link session is established	Peer MLAG member port is configured	Local MLAG member port is up	Peer MLAG member port is up
INIT	-	-	-	-
IDLE	-	-	-	-
DOWN	√	-	-	-

MLAG Interface State	Peer link session is established	Peer MLAG member port is configured	Local MLAG member port is up	Peer MLAG member port is up
INIT	-	-	-	-
IDLE	-	-	-	-
STANDBY	√	-	√	-
AS_DOWN	√	√	-	-
AS_PEER	√	√	-	√
AS_LOCAL	√	√	√	-
FULL	√	√	√	√

You can use the **run show mlag link** {*<link-id>***| summary**} command to view the state of the MLAG interface. For example,

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

In the output, **Link Status** shows the MLAG interface state, **Local Status** shows the status of local MLAG member port.

MLAG Control Plane Messages

The MLAG provides MLAG control plane messages, which is used to transmit the following information between the MLAG peer devices:

- MLAG state information.
- Synchronization information (including STP information synchronization and multicast control information synchronization).
- Configuration consistency check.

The MLAG control plane messages can be divided into two categories: L2 and TCP packets.

- For L2 packet, the destination MAC is 01:80:C2:00:00:0F and EtherType is 0x6666.
- For TCP packets, the destination port is 0xE290.

The format of MLAG control plane messages common header is:

Field	Descriptions
Version	This field specifies the MLAG version. Currently, the version is 0x1.
Type	This field specifies the type of MLAG control plane messages. • 0x1 indicates MLAG Control message. • 0x2 indicates MAC Sync message. • 0x3 indicates STP Sync message. • 0x5 indicates Multicast Control Sync message. • 0x6 indicates Configuration Consistency message.

MLAG control message includes the following four types and MAC Synchronization message:

- **MLAG Control message**

The MLAG Control message is used to maintain the MLAG status.

MLAG device sends an MLAG Control message under the following conditions:

1. MLAG neighbor state changes to ESTABLISHED.
2. Any MLAG interface state changes.

MLAG Control messages are encapsulated and transmitted via TCP protocol.

- **STP Sync**

The STP Sync message is used to sync up STP dynamic information, such as the calculated root priority and link cost from the received BPDUs to the peer switch. The STP Sync message is encapsulated and transmitted via TCP protocol.

- **Multicast Control Sync**

The Multicast Control Sync message is used to sync up IGMP/PIM dynamic information from the received IGMP/PIM message to the peer switch. The Multicast Control Sync message is encapsulated and transmitted via TCP protocol.

IGMP sees the MLAG LAG link as a unique logical link, so IGMP packets are synced between the MLAG peer devices through peer-link by Multicast Control Sync message:

IGMP packet received by either of the MLAG peer switches from MLAG port is synced to the other peer switch through peer link as if it is received by local MLAG port.

- **Configuration Consistency**

The Configuration Consistency message is used to check the MLAG related configuration consistency between MLAG peers. The Configuration Consistency message is encapsulated and transmitted via TCP protocol.

MLAG device sends a Configuration Consistency message under the following conditions:

1. A new MLAG related configuration is committed.

2. MLAG neighbor state changes to ESTABLISHED.

MAC Synchronization

In order to ensure that the traffic of the same user can be forwarded normally at both ends of the MLAG peer device, the MAC address table on both peer devices needs to be consistent with each other. This is accomplished by MAC synchronization mechanism which sends MAC synchronization message that is transferred by L2 multicast packets with destination address 01: 80: c2: 00: 00: 0f. MD5 checksum is added to the message to ensure that the MAC address table is correctly synchronized.

Meanwhile, in order to control bandwidth consumption of the MLAG peer link caused by flooding of unknown unicast traffic, the MLAG peer switches should synchronize MAC address table with each other.

Only when both of the following two conditions are satisfied, the MAC Sync message will be sent:

- MLAG neighbor state changes to ESTABLISHED.
- There is a change in the MAC table.

There are three types of MAC addresses defined in MLAG: Static, Dynamic, and Peer-Sync, where Peer-Sync represents the dynamic MAC address synchronized from the MLAG peer device, and its priority is lower than that of static MAC. If one of the MLAG peer switch fails, the Peer-Sync MAC address on the other switch will be deleted from the MAC address table.

Static and learned MAC addresses from any port except the peer link port are synced to MLAG peer switch through peer link. The MLAG peer's system MAC address which is learned on peer link is internally configured as static MAC address. New learned MAC addresses are immediately synced to the peer switch.

- How to update the MAC table with synced MAC addresses:
  - The MAC addresses learned on the single-homed port are synced to peer link port of the peer switch on the peer link.
  - The mac addresses learned on the MLAG member port are synced to the respective MLAG member port of the peer device through the MLAG peer link.
  - System MAC will be synchronized to the peer switch MLAG peer-link port as a **static** MAC address.
  - The MAC addresses learned on the peer link port are not synced.
- How to define the type of the MAC addresses:
  - If a MAC address is not statically configured but only learned on local MLAG switch, it is marked as "Dynamic" on local switch and "Peer-Sync" on peer switch.
  - If a MAC address is not statically configured but learned on both MLAG peer switches, it is marked as "Dynamic" on Node 0 switch and "Peer-Sync" on Node 1 switch.
  - Static MAC address has a higher priority so that it is not overridden by "Dynamic" and "Peer-Sync" MAC, but can override the "Dynamic" and "Peer-Sync" MAC types .
  - Static MAC addresses are not synced automatically, they should be synced manually.
  - If a static MAC address bound to a single-homed port is configured on one MLAG device, the static MAC address entry should be manually configured to bind to the peer-link interface on peer switch.
  - If a static MAC address bound to an MLAG member port is configured on one MLAG device, the static MAC address entry should be configured to bind to the MLAG member port on peer switch.
- How the MAC addresses age out:

  If the MAC addresses (Dynamic or Peer-Sync) age out or are cleared by CLI command on one of the MLAG peer devices, it is synced to the peer switch and removed from the peer switch as well.

You can use the **run show mac-address table** command to view the information about MAC address table, such as MAC address statistics, VLAN ID, MAC address, MAC address type and outbound interface.

For example,

Figure 4. A MAC Sync Example

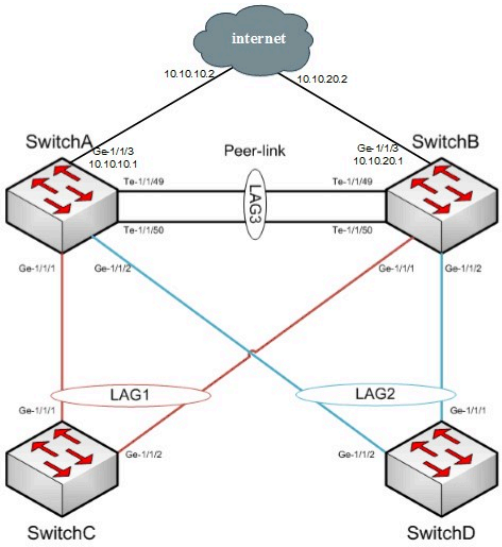
When showing the MAC table on Switch A and Switch B, we can see that the dynamic MAC entry learned from the MLAG member port will be synchronized to the corresponding MLAG member port on the peer device, and dynamic MAC learned from the single-homed port will be synchronized to the peer-link port on the peer device.

```
admin@SwitchA# run show mac-address table
Total entries in switching table:   3
Static entries in switching table:  0
Dynamic entries in switching table: 3

VLAN      MAC address           Type         Age      Interfaces         User
----      -----------------     ---------    ----     ----------------   ------
1         08:9e:01:61:64:13     Dynamic      300      ge-1/1/2           xorp
1         cc:37:ab:4f:ad:01     Peer-Sync    300      ae1                xorp
4088      8c:ea:1b:88:5b:81     Static       300      ae3                xorp

admin@SwitchB# run show mac-address table
Total entries in switching table:   3
Static entries in switching table:  0
Dynamic entries in switching table: 3

VLAN      MAC address           Type         Age      Interfaces         User
----      -----------------     ---------    ----     ----------------   ------
1         08:9e:01:61:64:13     Peer-Sync    300      ae3                xorp
1         cc:37:ab:4f:ad:01     Dynamic      300      ae1                xorp
4088      8c:ea:1b:88:5b:82     Static       300      ae3                xorp
```

When VXLAN is deployed in an MLAG domain, MAC sync between MLAG peer devices is different.

As shown in the following figure, the switches on the access side, SwitchC and SwitchD, are dual-homed to an MLAG domain. At the same time, a VXLAN tunnel is established between MLAG peer device SwitchA and SwitchB, so that Layer 2 devices on the access side can communicate over Layer 3 networks.

Figure 5. MLAG Topology with VXLAN



In this application, the MAC synchronization process is,

- The MAC addresses learned on the local network side port (Ge-1/1/3) are synced to the respective network side port (Ge-1/1/3) of the peer device through the MLAG peer link, as the system regards the network side ports on SwitchA and SwitchB as the same port.
- The MAC addresses learned on the local access side port, the MLAG member port in the figure, are synced to the respective access side port of the MLAG peer device through the MLAG peer link.
- MAC addresses learned on the single-homed port will not be synced to the peer-link port of the remote MLAG Node except in the following two cases.
  - When MLAG interface state is AS_LOCAL, the MAC addresses learned on the local access side port, the MLAG member port in the figure, are synced to the peer-link port of the MLAG peer device.
  - If the network port on one VTEP device goes down, the corresponding network on the peer VTEP is regarded as a single port and the MAC addresses learned this single port will be synchronized to the peer-link port of the MLAG peer device.

When showing the MAC address table, the value in **Interfaces** column is ***vxlan*** for MAC addresses synced from the peer VTEP device. For example,

```
admin@Xorplus# run show mac-address table
Total entries in switching table:   3909
Static entries in switching table:  6
Dynamic entries in switching table: 3903
VLAN      MAC address          Type         Age     Interfaces         User
----      -----------------    ---------    ----    ----------------   ----------
1         20:04:0f:0f:49:d1    Dynamic      300     ae2                xorp
N/A       00:00:0a:11:11:11    Peer-Sync    300     vxlan              xorp
N/A       00:00:0a:11:11:12    Peer-Sync    300     vxlan              xorp
```

You can also use command **run show vxlan address-table** to show VXLAN MAC table. For example,

```
admin@Xorplus# run show vxlan address-table
VNID           MAC address          Type       Interface      VTEP
-------------------------------------------------------------------------------------
10000          00:00:0a:11:11:11    Sync                      145.145.145.145
10000          00:00:0a:11:11:12    Sync                      145.145.145.145
10000          20:04:0f:0f:49:d1    Sync         ae2
```

The first two lines in the display result show the MAC addresses synced from the VXLAN network side port of the peer VTEP device, and the third line shows the MAC address synced from the access side port of the peer VTEP device.

Configuration Consistency Check

To ensure that the MLAG peer devices appear as one device to the downstream device, and to make the MLAG function operate normally and smoothly, the configuration on each MLAG peer device needs to be consistent.

PICOS automatically checks the configuration consistency of the MLAG peer devices by exchanging Configuration Consistency messages.

MLAG device sends a Configuration Consistency message under the following conditions:

- MLAG neighbor is established.
- An MLAG related new configuration is committed.

Configuration consistency check is divided into two types: **Global configuration** and **Per MLAG configuration**.

Global configuration refers to the global configuration of the MLAG module, STP module, DHCP snooping module and the IGMP snooping module. The configuration inconsistency affects the overall establishment and operation of the MLAG domain, the peer-link establishment, and the entire network topology. **Per MLAG configuration** is mainly for the configuration of a single MLAG. Inconsistent configuration only affects the establishment and operation of a single MLAG, but does not affect other MLAGs.

Depending on the impact of the configuration inconsistency on the system and the different MLAG processing methods, the consistency parameters are divided into six categories: **type 1**, **type 2**, **type 3**, **type 4**, **type 5** and **type 6**.

Type 1 Configuration Consistency Parameters

Table 1 shows all the type 1 parameters. When these parameters are inconsistent on MLAG peer, it might result in a traffic loop or losing MAC SYNC events of MLAG. A warning log will be generated to alert the users. Meanwhile,

- If the type 1 parameter is Global, MLAG will turn down all the MLAG member ports on the secondary spine (node ID= 1), regardless whether the corresponding MLAG member ports of the primary spine (node ID= 0) are up or down when these parameters are inconsistent on the MLAG peer.
- If the type 1 parameter is per MLAG type, MLAG will turn down only the MLAG port of the secondary spine, regardless whether the corresponding MLAG port of the primary spine is up or down when these parameters are inconsistent on the MLAG peer.

Table 1. Type 1 Configuration Consistency Check List

Configuration Parameter to Check	Type	Result When Inconsistent
Port settings (native vlan, trunk vlan count, trunk vlans)	Per MLAG	FAIL
PVST settings(root guard, vlan count, vlans, port priority, path cost)	Per MLAG	FAIL
MSTP settings(external path cost, internal path cost, port priority, mst count, msti, mst port priority, mst path cost, configuration name, revision level, vlan count, vlans)	Per MLAG	FAIL
RSTP/PVST/MSTP enable or disable	Global	FAIL
RSTP/PVST/MSTP mode	Global	FAIL

Type 2 Configuration Consistency Parameters

Table 2 shows all the type 2 parameters. When these parameters are inconsistent, it does NOT cause a loop or MAC SYNC issue. However, some traffic may be impacted. A warning log will be generated to alert the users when these parameters are inconsistent on the MLAG peer.

Note that VXLAN settings belongs to both type 2 and type 6, when these parameters are inconsistent, the check result is "FAIL".

Table 2. Type 2 Configuration Consistency Check List

Configuration to Check	Type	Result When Inconsistent
MLAG link ID	Global	ALERT
MLAG link count	Global	ALERT
MLAG peer VLAN	Global	ALERT
MTU	Global	ALERT
LACP priority	Global	ALERT
LACP key	Global	ALERT
MAC learning	Global	ALERT
Port LAG mode (LACP/Static)	Global	ALERT
Port mode (Access/Trunk)	Global	ALERT
RSTP settings (BPDU filter, BPDU Guard, Edge, Root Guard, TCN Guard, Bridge priority, Max age, Hello time, Forward delay, Link type, Port priority, Path cost)	Global/Per MLAG	ALERT
PVST settings (VLAN count, VLANs, Bridge priority, Hello time, Forward delay, Max age, BPDU guard, Manual forwarding, Link type)	Global/Per MLAG	ALERT
MSTP settings (BPDU filter, BPDU Guard, Edge, Root Guard, TCN Guard, Bridge priority, Max age, Hello time, Forward delay, Link type, Path cost, Max hops, VLANs, Manual forwarding)	Global/Per MLAG	ALERT
VXLAN settings (UDP port, MAC learning, VXLAN enable, vni count, vni to vlan mapping, vni to vtep count, vni to vteps, vni count, vnis, vni to vlan count, vni to vlans)	Global/Per MLAG	FAIL
IGMP snooping vlan count, IGMP snooping vlans	Global	ALERT

Type 3 Configuration Consistency Parameters

Table 3 shows all the type 3 parameters. When these parameters are inconsistent, a loop may be formed. In some cases, turning down the MLAG port is not enough to prevent the loop. Hence, if a type 3 parameter is inconsistent, all VLANs (except MLAG peer VLAN) on the peer link will be blocked to prevent the loop. Also, a warning log will be generated to alert the users. The log will repeat every 60s until the configuration is modified to be consistent.

Table 3. Type 3 Configuration Consistency Check List

Configuration to Check	Type	Result When Inconsistent
MLAG domain ID	Global	FAIL
RSTP/PVST/MSTP enable or disable	Global	FAIL
RSTP/PVST/MSTP mode	Global	FAIL

Type 4 Configuration Consistency Parameters

Table 4 shows all the type 4 parameters. When these parameters are inconsistent, MAC addresses will not be synchronized between MLAG peer devices.

Table 4. Type 4 Configuration Consistency Check List

Configuration to Check	Type	Result When Inconsistent
MLAG domain ID	Global	FAIL

Type 5 Configuration Consistency Parameters

Table 5 shows all the type 5 parameters. When these parameters are inconsistent, only MSTP parameters in instance 0 can be synchronized between MLAG peer devices.

Table 5. Type 5 Configuration Consistency Check List

Configuration to Check	Type	Result When Inconsistent
MSTP settings(configuration name, revision level, vlan count, vlans)	Global	FAIL

Type 6 Configuration Consistency Parameters

Table 6 shows all the type 6 parameters. It will stop DHCP table sync between the MLAG peer when any of the following DHCP snooping configurations inconsistency are detected: dhcp snooping vlan count, dhcp snooping vlans.

Table 6. Type 6 Configuration Consistency Check List

Configuration to Check	Type	Result When Inconsistent
DHCP snooping (vlan count, vlans)	Global	FAIL
VXLAN settings (UDP port, MAC learning, VXLAN enable, vni count, vni to vlan mapping, vni to vtep count, vni to vteps, vni count, vnis, vni to vlan count, vni to vlans)	Global/Per MLAG	FAIL

NOTEs:

- Some parameters belong to two types, for example, parameter "RSTP/PVST/MSTP enable or disable" belongs to both type 1 and type 3. When this configuration is inconsistent, MLAG will take actions necessary for both type 1 and type 3 inconsistencies.
- VXLAN settings belongs to both type 2 and type 6,
  - When VXLAN is deployed simultaneously with DHCP snooping, it will stop DHCP table sync between the MLAG peer when any of the VXLAN settings in **Table 6** are inconsistent on the MLAG peer devices.
  - When VXLAN deployment is independent of DHCP snooping, a warning log will be generated to alert the users when VXLAN settings parameters are inconsistent on the MLAG peer devices.
- If “domain ID” inconsistency is detected, all VLANs (except MLAG peer VLAN) on the peer link will be blocked to prevent the network loop. And also, MAC synchronization will not be performed between the MLAG peers until the configuration is modified to be consistent. A warning log will be generated to alert the users.
- When any of the following MSTP configurations inconsistency is detected: configuration name, revision level, mst count, msti, vlan count, MSTP only uses parameters of instance zero from peer to prevent loop. A warning log will also be generated to alert the users.

To ensure that the configuration parameters are consistent, we recommend that you run the MLAG consistency check command to display the configurations and the consistency check results for each MLAG peer device once you set a new MLAG related configuration.

You can use the **run show mlag consistency-parameter** {**link** <*link-id*>| **summary**} command to view the consistency check results. For example:

```
admin@Xorplus# run show mlag consistency-parameter summary
Overall : PASS with ALERT
--------------
Global  : PASS with ALERT
Link 1  : PASS with ALERT

MLAG Configurations:
----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Domain ID               1                1                PASS
Node ID                 0                1                PASS
Peer VLAN               33               4094             ALERT
Link Count              1                1                PASS
Link IDs                1                1                PASS

Spanning-Tree Configurations:
----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  Yes              Yes              PASS
Mode                    RSTP             RSTP             PASS
Bridge Priority         0                32768            ALERT
Hello Time              3                2                ALERT
Forward Delay           5                15               ALERT
```

```
Max Age                  7               20              ALERT

DHCP Snooping Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
VLAN Count               0               0               PASS
VLAN IDs                                                 PASS

IGMP Snooping Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
Enable                   No              No              PASS

VXLAN Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
VXLAN UDP Port           4789            4789            PASS
VXLAN Mac Learning       TRUE            TRUE            PASS
VXLAN Enable             TRUE            TRUE            PASS
VXLAN Source VTEP        10.226.14.254   10.226.14.254   PASS
VXLAN VNI Count          10              10              PASS
VXLAN VNIs                                               PASS


admin@Xorplus# run show mlag consistency-parameter link 3
Port Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
MTU                      1514            1514            PASS
Mac Learning             Yes             Yes             PASS
Lag Mode                 LACP            LACP            PASS
Native Vlan              3               3               PASS
Port Vlan Mode           Access          Access          PASS
Trunk Vlan Count         2               2               PASS
Trunk VLAN IDs                                           PASS


Spanning-Tree Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
Mode                     PVST            PVST            PASS
BPDU Guard               No              No              PASS
Root Guard               No              No              PASS
Manual Forwarding        No              No              PASS
Link Type                P2P             P2P             PASS
Instance Count           1               1               PASS
Instance Vlan 3
-- Port Priority         128             128             PASS
-- Path Cost             0               0               PASS

VXLAN Configurations:
------------------------------------------------------------------
Property                 Local Value     Peer Value      Result
-----------------------  --------------  --------------  ------
Link   1 VXLAN           N/A             N/A             FAIL
```

Result in the show commands shows the consistency check results, the value could be **PASS**, **FAIL** or **ALERT**:

- If **Result** is PASS, the configurations of the MLAG peer-link devices are consistent.
- If **Result** is FAIL or ALERT, the configurations of the MLAG peer-link devices are inconsistent.

In the consistency check results,

- if there exists one "FAIL" result, the "Overall" result would be "FAIL".
- Else, if there exists one "ALERT" result, the "Overall" result would be "ALERT".
- Else, the "Overall" result would be "PASS".

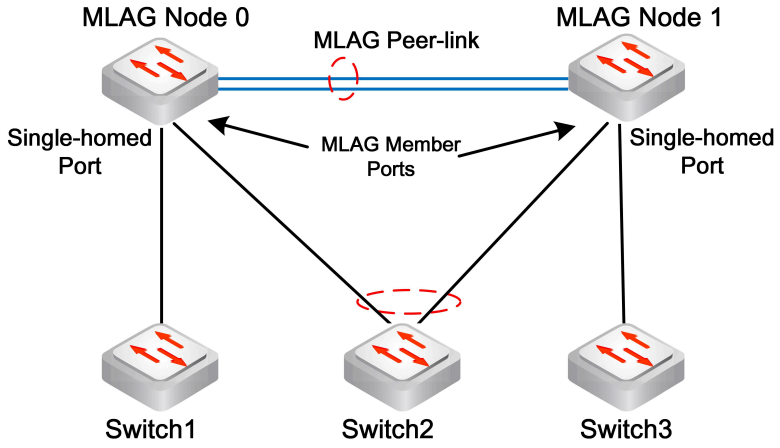
NOTE:

- Inconsistent configurations may cause MLAG to run abnormally.
- After the configuration is changed from inconsistent to consistent, you need to restart the MLAG peer devices to ensure that MLAG functions normally.

Single-homed Port

Single-homed port is a port on the MLAG peer device which provides access device single-access to the network through either MLAG Node 0 or Node 1 device. The single-homed port on the MLAG peer devices can connect to both hosts or servers and it can also be connected to other access switch devices. As shown in **Figure 6**, Switch 1 and Switch 3 are single-homed devices, the ports on the MLAG peer devices connected to Switch 1 and Switch 3 are called single-homed ports. Traffic between Switch1 and Switch3 always crosses the MLAG peer-link as Switch1 and Switch3 are active on different switches. With single-homed ports, servers and other standalone switches are able to single-home into the network.

Figure 6. MLAG network



The MAC address entries learned on the single-homed port will be synchronized to the MLAG peer-link port on the MLAG peer device, and the address type is **Peer-Sync** in the MAC address table. However, the MAC synchronization on the single-homed port will be done only when the MLAG neighbor state is ESTABLISHED. This MAC synchronization ensures that the devices connected to the single-homed port can communicate normally.

Physical ports and LAG ports could be a single-homed port, an MLAG member port matching the following conditions could be a single-homed port, but the peer-link port could not be a single-homed port.

An MLAG member port is a single-homed port when one LAG port of the dual-homed access device is down, then the other LAG port becomes a single-homed port. We can also say that when MLAG interface state is **ASY_LOCAL**, then MLAG member port on local MLAG device is a single-homed port. MAC address entry learned on this port will be synchronized to MLAG peer-link port on the MLAG peer device.

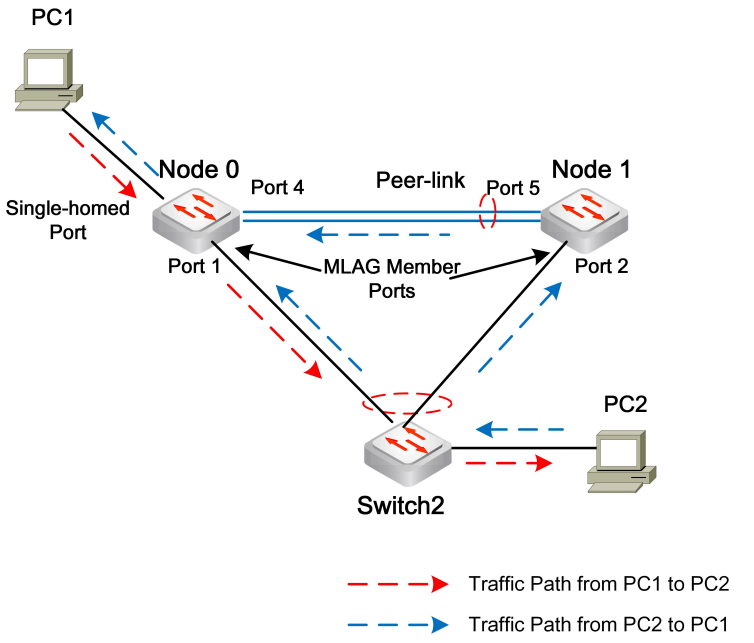
NOTE:

To make the single-homed port work normally, the peer-link ports should be added into the VLAN of the single-homed port.

Application Scenarios

As shown in **Figure 7**, PC 2 connects to the MLAG downlink switch (Switch 2), and communicates with PC 1 through the MLAG peer devices.

Figure 7. Network 1 of PC 1 and PC 2 Communication in MLAG Topology



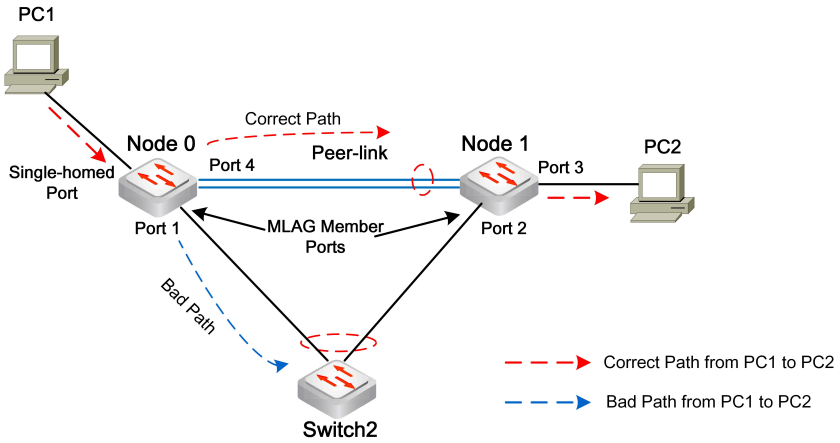
Normally, the traffic from PC 1 to PC 2 will go out through Port 1 to Switch 2. Any packet received from peer-link on MLAG Node 1 device will be blocked on all MLAG member ports.

Traffic sent from PC 2 to PC1 will be hashed to one of the MLAG peer devices. If the traffic is hashed to the MLAG Node 1, the traffic is therefore forwarded by the Node 1 device across the peer-link to MLAG Node 0. This is because the MAC address learned on the single-homed port will be synchronized to the peer-link port Port 5 on MLAG Node 1 device.

When the topology changes, as shown in **Figure 8**, PC 2 changes location and accesses the network through the MLAG Node 1 on Port 3. The MAC address of PC 2 will be learned on Port 3 of MLAG Node 1 device. At this time, since Port 3 is a single-homed port, the MAC address entry learned on Port 3 will be synchronized to the peer-link port Port 4 on MLAG Node 0 device. The traffic sent from PC 1 to PC 2 will go out of Port 4 instead of Port 1 on MLAG Node 0 device and sent to the Node 1 device via peer-link.

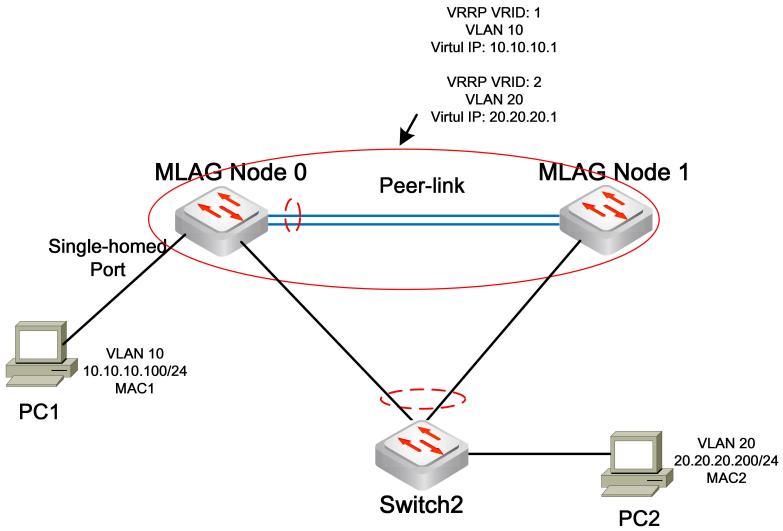
Similarly, as Port 3 is a single-homed port, MAC addresses of single-homed hosts connected to the MLAG Node 1 device will automatically be learned by MLAG Node 0 device. The traffic flow path from PC 2 to PC 1 is similar. This ensures that the devices connected to the single-homed port can communicate normally.

Figure 8. Network 2 of PC 1 and PC 2 Communication in MLAG Topology



When considering the case of IP routing communication, as shown in **Figure 9**, PC1 and PC2 belong to different subnets. In this scenario, you can apply VRRP in the MLAG topology to make PC1 and PC2 communicate with each other through IP routing. Configure two VRRP groups on the two VRRP group devices which belong to different L3 VLAN interfaces. Configure a different virtual IP address for each VRRP group, virtual IP address 10.10.10.1 is used as the gateway for PC1 access network, and virtual IP address 20.20.20.1 is used as the gateway for PC2 access network.

Figure 9. Network 3 of PC 1 and PC 2 Communication in MLAG with VRRP Topology



If VXLAN is deployed in an MLAG domain, MAC addresses learned on the single-homed port will not be synced to the peer-link port of the remote MLAG Node except in the following two cases.

- When MLAG interface state is AS_LOCAL, the MAC addresses learned on the local access side port, the MLAG member port in the figure, are synced to the peer-link port of the MLAG peer device.
- If the network port on one VTEP device goes down, the corresponding network on the peer VTEP is regarded as a single port and the MAC addresses learned this single port will be synchronized to the peer-link port of the MLAG peer device.

Flood Control

To prevent the downstream switches from receiving multiple copies from both ends of MLAG peer, a block mask is used to prevent forwarding all the traffics received on the MLAG peer link toward the MLAG member port, this is called Flood Control mechanism.

As shown in **Figure 10**, peer-link is usually not used to forward data traffic, the unicast traffic from the access device or the network side to the MLAG peer device will be forwarded locally. When receiving the traffic from the peer-link, the MLAG member ports start flood control and form a forwarding block mask. That is, traffic received from the peer-link port will not be forwarded out the MLAG port; this prevents loops in the MLAG network.

The forwarding block mask for a given MLAG will be cleared off if the MLAG member port goes down on the MLAG peer.

Figure 10. MLAG Flood Control

1. Unknown unicast, multicast or broadcast received from the MLAG member ports will be flooded to any other ports in MLAG VLAN including the peer-link port.
2. Any packets (Unicast, multicast or broadcast) received from peer-link will be forbidden to transfer through the MLAG member port.

You can run the **run show mlag link** {<link-id>**| summary**} command to view the status of flood control. For example:

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer-Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

In the show result, **Link Status** indicates MLAG interface state. Generally, **Flood** is **No**, indicates that all the traffic received on the MLAG peer-link port will be blocked to all MLAG member ports on MLAG peer device except the DHCP Offer/Ack packets.

However, in one case, when peer MLAG member port is down, the MLAG interface state changes to AS_LOCAL, then **Flood** changes to **Yes**, indicating that traffic received on the MLAG peer-link can be transferred through the MLAG member port.

> **NOTE:**
>
> All the packets received from peer-link shall be blocked to all MLAG member ports except the DHCP Offer/Ack packets.

MLAG Peer-Gateway

As shown in the figure below, Switch 1 and Switch 2 are a pair of MLAG devices. The host can dual-access to the network through the MLAG peer devices. VRRP is not deployed in this topology.

Let's assume that the default gateway address on the host is the address of Switch 2. In this case, any message from the host directly sent to Switch 2 can be routed correctly. However, there may exist one case that message from the host is hashed to Switch 1, Switch 1 finds that the destination MAC address of the message is Switch 2, then the message will be forwarded to Switch 2 through the peer link. When the message received from the peer link is about to be forwarded on the MLAG member port on Switch 2, it will be dropped due to MLAG flood control mechanism.

To solve this problem, you can enable Peer-Gateway functionality on both sides of the MLAG devices. Each MLAG local device will then replicate the system MAC address of the peer MLAG device, allowing the local device to function as a gateway to forward packets destinated for the MLAG peer device.

In the scenario above, when Switch 1 receives a message in which the destination MAC is the system MAC address of the peer MLAG device Switch 2, which is also the gateway MAC of the host, Peer-Gateway feature allows the local MLAG device Switch 1 to function as the gateway for forwarding message. This avoids forwarding message through the peer link, avoiding packet drops on Switch 2 due to MLAG flood control mechanism.

You can use the command **set protocols mlag domain** <*domain-id*> **peer-gateway enable** <**true** | **false**> to enable or disable MLAG Peer-Gateway functionality.

For example,

- Enable MLAG Peer-Gateway functionality.

```
admin@Xorplus# set protocols mlag domain 1 peer-gateway enable true
admin@Xorplus# commit
```

- Disable MLAG Peer-Gateway functionality.

```
admin@Xorplus# set protocols mlag domain 1 peer-gateway enable false
admin@Xorplus# commit
```

When MLAG Peer-Gateway is enabled on the MLAG peer devices, where DHCP Relay is also enabled, you have to configure an IP address of the DHCP relay agent through the command **set protocols dhcp relay interface** <*vlan-interface-name*> **relay-agent-address** <*agent-ipv4-address*>. In this command, **interface** <*vlan-interface-name*> is the VLAN interface with DHCP relay enabled; **relay-agent-address** <*agent-ipv4-address*> needs to be configured as an IP in the same network segment as the VLAN interface but a different value. Note that the DHCP relay agent address should be identical on both MLAG peer devices.

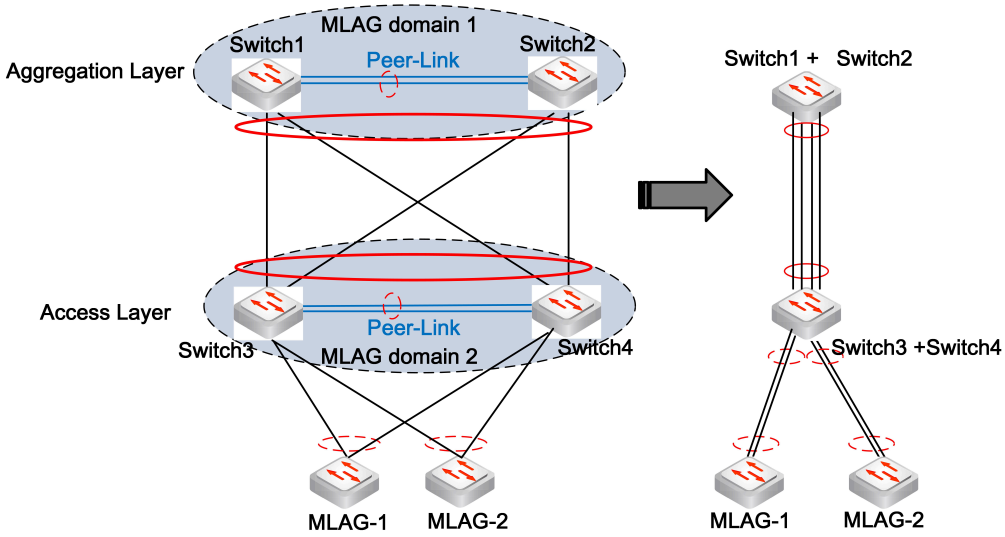
Multi-layer MLAG Application Networking

A two-layer MLAG network is shown in **Figure 11**. Access devices dual-homed to the network through the lower MLAG peer devices at the access layer, and the upper MLAG peer devices are used as the active-active gateway at the aggregation layer. In the two-layer MLAG topology, MLAG member ports of the MLAG peer device in the same MLAG domain MUST belong to the same MLAG, that is, they should be configured with the same link ID.

NOTE:

It is mandatory that different pairs of MLAG peer devices should use different domain IDs. In the topology below, domain ID of Aggregation Layer MLAG peer switches and domain ID of Access Layer MLAG peer switches should be different.

Figure 11. Multi-layer MLAG Application Networking Diagram



Compared with one layer MLAG, multi-layer MLAG has the following advantages:

- Expanded layer 2 range.
- Provides a highly flexible architecture. In the multi-layer MLAG, both access devices and access layer switches devices are dual-homed to the network, which increases network reliability.

Provides greater network bandwidth from the access layer to the aggregation layer.

Interoperability with Other Features

LACP

LAG (Link Aggregation Group) is a way of binding multiple physical links into a combined logical link. MLAG domain MAC address will be used for LACP negotiation when performing link aggregation with the downlink access device.

We recommend that you enable LACP on the interfaces of each link aggregation group when configuring peer-link port and the LAG ports connected to the downlink access devices. This allows you to more easily detect compatibility between devices, link failures, and provides dynamic reaction to configuration changes and link failures.

Rapid PVST+

MLAG itself has an anti-loop feature for MLAG member ports, but for non-MLAG ports, the possibility of a loop still exists in the network. There could be a number of networking scenarios that could lead to loops in the network, so to avoid unexpected loops forming in the network, it is strongly recommended to enable Rapid PVST+ protocol on all devices in the MLAG domain.

The two MLAG peer switches are seen as a single device to the PVST+ instance. Rapid PVST+ configuration should be identical on both MLAG peer devices. For example, rapid PVST+ enable or disable, rapid PVST+ mode and rapid PVST+ parameters (such as bridge priority, hello time, forward delay) should be identical on both MLAG peer devices.. See Table 1 in section 1.1.6 Configuration Consistency Check to find the MLAG configuration consistency check list.

After the rapid PVST+ protocol is enabled, MLAG peer devices will automatically send STP Sync messages, which are used to sync up rapid PVST+ dynamic information from the received BPDUs to the peer switch. Once the peer-link is successfully established, the two peers are virtualized into one device to perform port role calculation and fast convergence calculation by using the rapid PVST+ protocol. The peer link port is always in forwarding state and does not participate in the spanning tree calculation.

NOTE: To avoid network loop, it is strongly recommended all the VLANs on the peer-link port to enable with rapid PVST+, including MLAG peer VLAN.

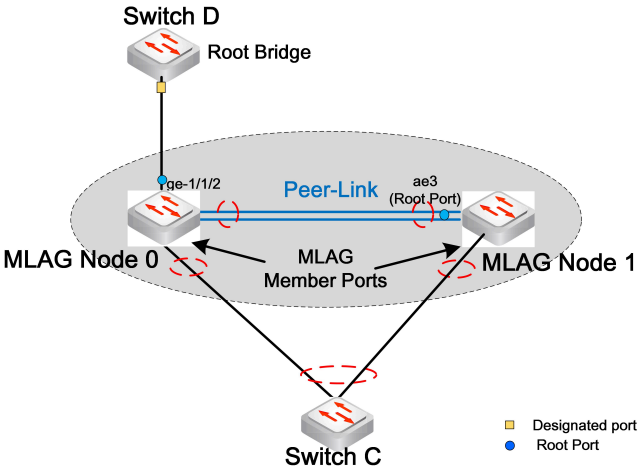
An offset has been added to the port index which is encapsulated in the BPDUs, see the following table:

	MLAG Port Index	Non-MLAG Port Index
MLAG Node 0	512 + MLAG Link ID	Local Port Index
MLAG Node 1	512 + MLAG Link ID	1024 + Local Port Index

Supported Root Bridge Topologies

Root bridge could be any bridge in the L2 domain, connected through the following three types of link:

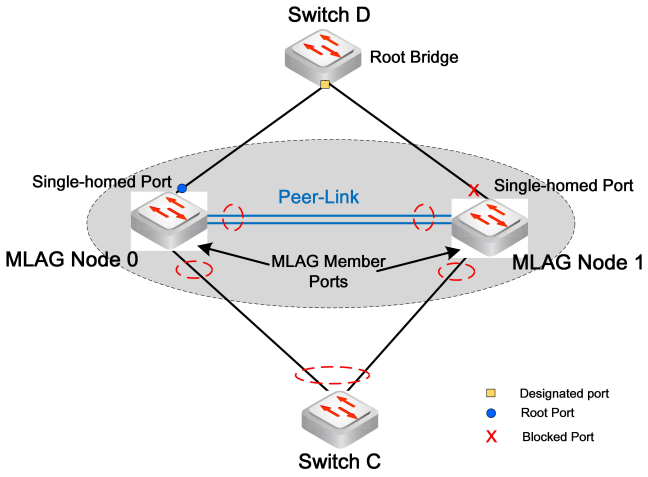
1. Non-MLAG link, i.e. single-homed connection to either one or both of the peer nodes.



In the figure above, Switch D is single-homed to MLAG Node 0 device, suppose Switch D is the root bridge, then ge-1/1/2 port is the root port of MLAG Node 0, and the peer-link port ae3 is the implicit root port of MLAG node 1 device.

In the figure above, Switch D is single-homed to both MLAG Node 0 and Node 1 devices. Suppose Switch D is the root bridge, in the upper side of the topology, one of the single-homed ports will be blocked after spanning tree calculation as there is a loop in the topology.

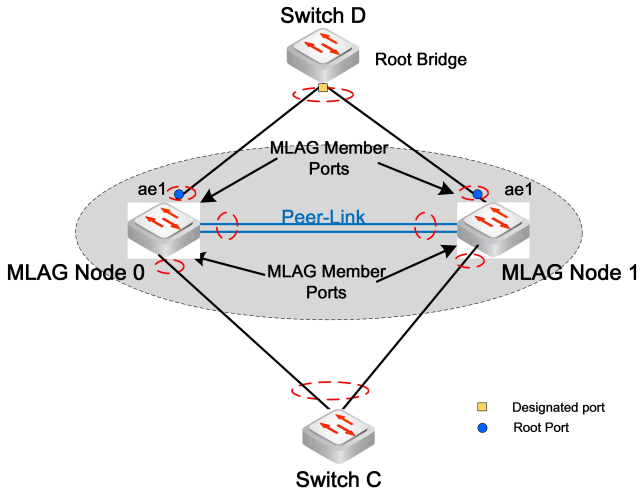
2. MLAG link



In the figure above, Switch D is dual-homed to MLAG peer devices, suppose Switch D is the root bridge, LAG port ae1 is the root port of MLAG Node 0. After STP synchronization between MLAG peer devices, LAG port ae1 becomes the root port of MLAG node 1 device.

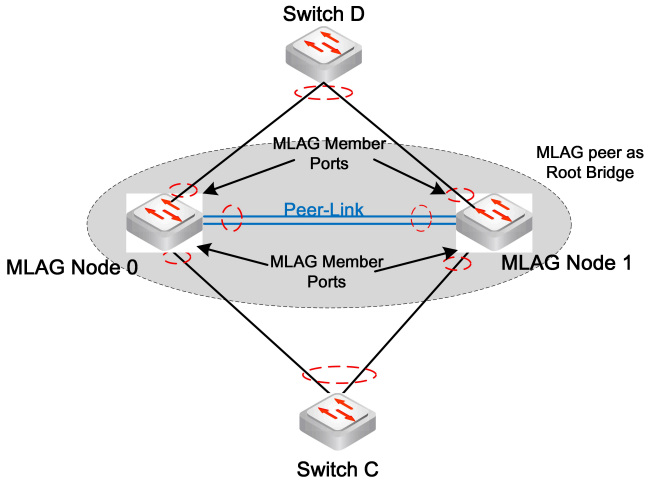
If one of the MLAG member port goes down, the role of paired MLAG member port remains unchanged in the MLAG domain.

For example,



In the figure above, if the MLAG member port ae1 on MLAG Node 0 goes down, the role of the paired MLAG member port in the MLAG domain is still the root port.

3. MLAG nodes as the root bridge



In the figure above, Switch C and Switch D are dual-homed to MLAG peer devices, MLAG peer devices functions as a root bridge. One of the MLAG peer devices transmits configuration BPDUs.

Configuration recommendation:

- For a small scale network, it is recommended to disable spanning tree protocol to reduce the network convergence delay caused by spanning tree calculation.
- If the network topology changes, MAC address table will be cleared.

DHCP Snooping & DHCP Relay

Devices in the MLAG topology support enabling DHCP snooping or DHCP relay function on the MLAG peer devices to implement address allocation for the DHCP clients.

When configuring DHCP snooping and DHCP relay in MLAG topology, pay attention to the following points:

- DHCP snooping configurations, such as Option 82 policy, VLANs enabled or disabled DHCP snooping, should be configured identically on both MLAG peer devices, the inconsistent configuration can cause undesirable behavior in the traffic flow.
- If the VLANs enabled or disabled DHCP snooping are not identical on MLAG peer devices or the MLAG global configuration are not identical on MLAG peer devices, the DHCP binding table entries will be cleared.
- When configuring DHCP snooping, the ports directly or indirectly connect the DHCP server should be configured as trust port on the network device between the DHCP Client and the Server, including the MLAG peer devices.
- DHCP relay configurations should be configured identically on both MLAG peer devices.

DHCP snooping and DHCP relay in MLAG topology present the following characteristics:

1. DHCP snooping binding table and DHCP relay table of the MLAG member ports will be synchronized to the associated member ports on MLAG peer device. DHCP Sync message is defined to undertake the synchronization tasks.
2. If the MLAG configuration consistency check passes, the MLAG system syncs the DHCP snooping binding table and DHCP relay table; If the MLAG configuration consistency check fails, the MLAG system does not sync the DHCP snooping binding table and DHCP relay table.
3. DHCP snooping binding table and DHCP relay table of the single-homed ports will not be synchronized to the MLAG peer device.
4. When receiving the DHCP message from MLAG peer link, the MLAG device won't do Layer 3 forwarding for this message, but can do Layer 2 forwarding.
5. MLAG flood control module processes DHCP packets just like other packets: When the MLAG member port is in the FULL state, DHCP packets received from the peer link port cannot be forwarded out from the MLAG member port; However, when the MLAG interface state changes to AS_LOCAL, the prohibition is lifted.
6. MLAG device forwards one copy of the DHCP Discover/Request/Release/Decline packet received from the MLAG member ports to the MLAG peer device through the peer link.
7. The format of DHCP Option 82 sub-options remote ID and circuit ID is fixed in MLAG topology,

- MLAG domain MAC address is used to fill in remote ID field.

- MLAG Link ID and Port Index are used for circuit ID field with an offset, see the following table for details:

	MLAG Port	Non-MLAG Port
MLAG Node 0	512 + MLAG Link ID	Local Port Index
MLAG Node 1	512 + MLAG Link ID	1024 + Local Port Index

IGMP Snooping

IGMP snooping can be deployed in an MLAG topology to shield hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. The multicast traffic is forwarded according to the L2 multicast forwarding table which is generated by IGMP snooping. If there is no matching entry in the L2 multicast forwarding table, the multicast traffic is forwarded to the mrouter ports except the one the multicast traffic is received on.

IGMP sees the MLAG LAG link as a single logical link, so IGMP packets are synced between the MLAG peer devices through peer-link by Multicast Control Sync message:

IGMP packet that is received on either MLAG peer switch from their MLAG port is synced to the other peer device through peer link as if it is received by local MLAG port.

Configuration notes:

- IGMP snooping configuration should be identical on both MLAG peer devices.
- Generally, it is not necessary to configure mrouter port on the peer link.

VXLAN

Implementing VXLAN technology on the MLAG peer devices provides overlay network on top of existing layer 2 and layer 3 technologies to support elastic compute architectures, thus makes it easier for network engineers to scale out a cloud computing environment while logically isolating cloud apps and tenants.

The two MLAG peer switches are seen as a single device in the VXLAN network. VXLAN configurations should be identical on each VTEP device. This includes the VNI value, VLAN included in the same VNI and all the configurations on the VXLAN network side ports and access side ports.

To avoid duplicate packets being sent from MLAG and VXLAN networks, traffic from the peer link will not be forwarded on the VXLAN network side ports or access sides ports, unless in the case that the uplink or downlink of the peer VTEP device fails.

When VXLAN is deployed in MLAG domain, pay attention to the following notes:

- When deploying VXLAN, peer link should not be the outcoming interface of VXLAN tunnel for routing VXLAN traffic, otherwise packet loss may occur.
- Untagged packets do not support VNI mapping to the PVID of a port by using command **set vxlans vni** *<text>* **vlan** *<vlan-id>*.
- In MLAG with VXLAN network, configuring static MAC address entries on VXLAN tunnel interfaces is not supported, so the command **set vxlans vni***<text>* **flood vtep** *<ipv4-addr>* **mac-address** *<macaddr> is useless.*
- Traffic from the single-homed port cannot be sent from the peer spine's network side port of VXLAN because of the limitation that the traffic from the peer link will not be forwarded through the VXLAN network side ports.
- Only one VLAN can be configured for one VNI when you use the command **set vxlans vni** *<text>* **vlan** *<vlan-id>* to configure the VLAN permitted to pass through the VXLAN tunnel.
- If the local VXLAN access port status is Down, packets from the VXLAN network side will be discarded on the local MLAG peer-link port if they become packets without a VLAN tag after VXLAN decapsulation.
- The single-homed port is not supported as VXLAN access port, only dual-homed MLAG member port can be configured as VXLAN access port.
- Only MLAG Node 0 device can forward the BUM packets through the VXLAN tunnel.

ARP Inspection

ARP Inspection can be deployed on the MLAG peers to defend against man-in-the-middle attack scenarios, preventing ARP table entry being maliciously modified by a forged ARP message sent by an attacker.

Configuration notes:

- ARP inspection configuration should be identical on both MLAG peer devices.
- We recommend the you don't enable ARP inspection in the peer-link VLAN which is dedicated to transmitting MLAG control plane messages.

However, if ARP inspection is enabled in peer link VLAN, an ARP access list must be configured by the following commands for ARP inspection to make MLAG work normally:

set protocols arp inspection access-list *<acl-name>* **ip** *<ipv4-addr>* **mac-address** *<mac-addr>*

set protocols arp inspection vlan *<peer-vlan-id>* **access-list** *<acl-name>*

where IP, MAC address and VLAN should be configured as the corresponding values of peer link port on the MLAG peer device.

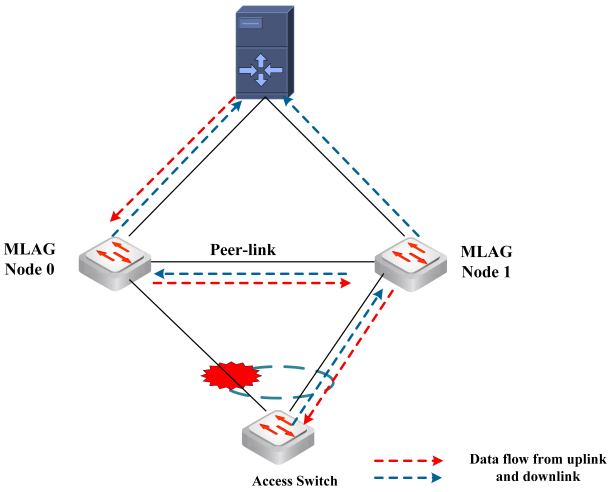
Traffic Forwarding in Typical Fault Scenarios

Downstream Link from Access Switch Down

This scenario includes the case in which an MLAG member port goes down or downstream link develops a fault. In this case, all traffic will be transmitted to and from the active MLAG member port of the peer device as illustrated in **Figure 12**.

From Figure 11, when the member port on Node 0 goes down, MLAG interface state on MLAG Node 1 changes to AS_LOCAL. MLAG member port on Node 1 becomes an MLAG single-homed port. Frames received from the peer link are then forwarded to the MLAG single-homed port.

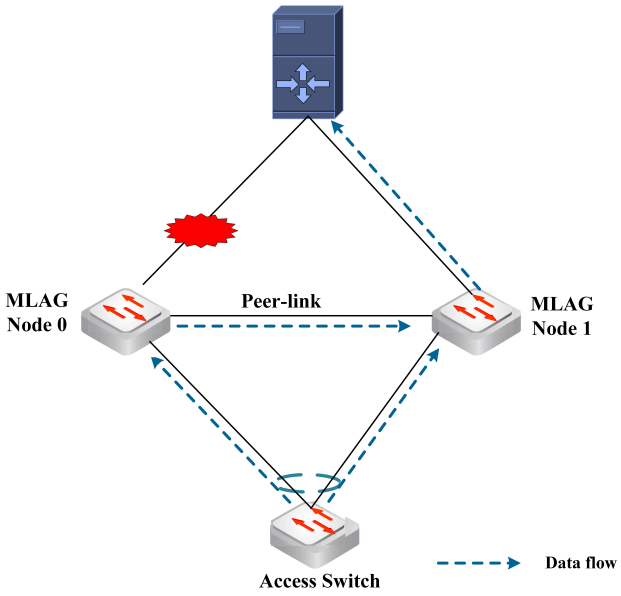
Figure 12. Typical Fault Scenario of Downstream Link Down



Upstream Link to Layer-3 Device Down

In this case, traffic load-sharing to MLAG Node 0 is sent to the MLAG Node 1 device via MLAG peer-link, and then forwarded to the upstream device.

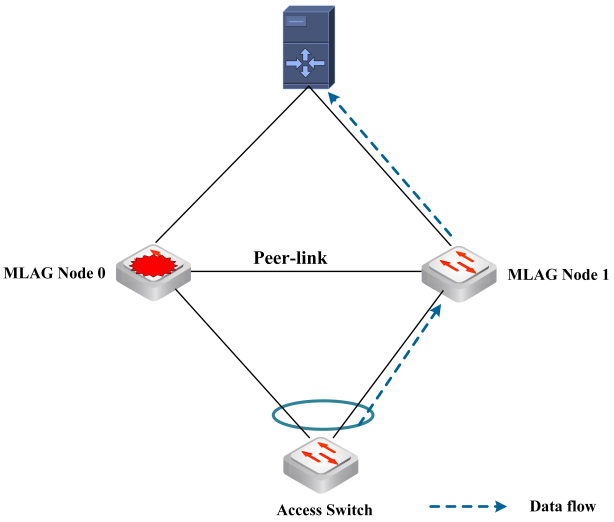
Figure 13. Typical Fault Scenario of Upstream Link Down



MLAG Node Fault

If one of the MLAG Node reboots, shuts down or develops some unforeseen fault, traffic will be transmitted through the other active MLAG Node.

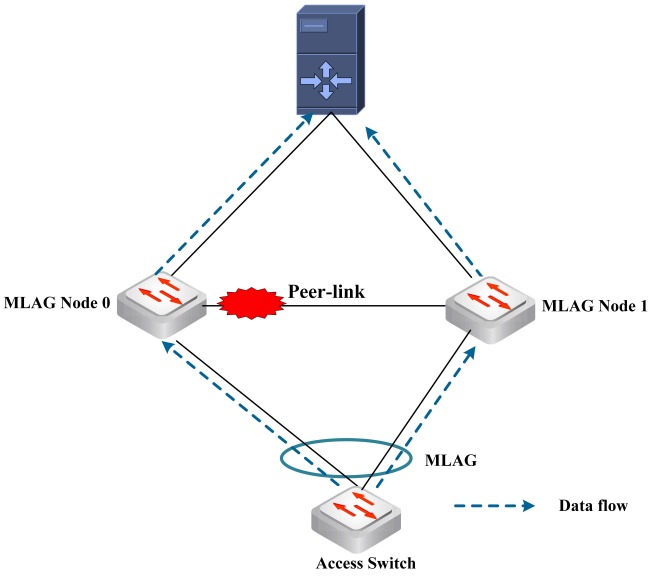
Figure 14. Typical Fault Scene of MLAG Node 0 Fault



MLAG Peer-link Down

Any manual action to shut down the peer-link is strictly forbidden. However, if the peer-link goes down for some reason, MLAG control plane messages cannot be exchanged, causing the MLAG system to operate abnormally. Especially when the peer-link is down, but both the MLAG member ports are up will create the split-brain failure scenario. The system cannot be automatically recovered in this scenario.

Figure 15. Typical Fault Scenario of Peer-link Down



Therefore, we have to ensure the reliability of the peer-link, follow the points described in section 1.1.2 Basic Concepts when configuring and deploying the peer-link.

When the peer-link is down, the MLAG peer relationship cannot be established. You can run the **run show mlag domain** command to check the peer-link status, the **Neighbor Status** is not ESTABLISHED when peer-link is in process of establishment or is down.

For example,

```
admin@Xorplus# run show mlag domain summary
Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 1
-------------------------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status    Config Matched       MAC Synced  # of Links
---------  ---------------  ---------  ---------------    --------------      ----------  ----------
ae65       1.1.1.1          4088        ESTABLISHED         Yes                Yes          64
```

Backward Compatibility

Compared with existing CLI interface, from 3.6.0, the new CLI is not backward compatibility as follows:

- “set interface mlag” is changed to “set protocols mlag”.
- “disable”/“hello-interval”/”priority”/“reload-delay”/”source”/”system-id” are obsoleted.
- “set interface aggregate-ethernet xx aggregated-ether-options mlag domain-id” is changed to “set protocols mlag domain xx interface xx link”.
- No MLAG link level “peer-ip” and “peer-link” anymore. Instead only global level configuration for all MLAG links within the same domain are provided.
- “set interface mlag peer x.x.x.x peer-link xx” is changed to “set protocols mlag peer-ip x.x.x.x peer-link xx”.

- By default, all existing MLAG configuration is moved under MLAG domain 1.

Compared with existing MLAG behavior, from 3.6.0, the major differences are as follows:

- No MLAG master/slave election. Instead the MLAG primary/secondary role is determined by the MLAG node configuration.
- No interval-based Hello message. Instead the MLAG Control message is triggered on-demand.
- The MLAG message encapsulation is changed from UDP to TCP.
- The MLAG message format is changed to TLV style.
- Configuration Consistency check is introduced and there is no more configuration sync from master to slave.
- MLAG state machine is changed more user friendly.
- MLAG domain MAC is always used in LACP and STP instead of master's MAC.
- When VXLAN is enabled, the peer link port is always set to access port.

Configuration Notes and Constraints

When configuring MLAG, pay attention to the following notes:

- When peer-link is down, but both the MLAG member ports are up, the split-brain failure scenario occurs. The MLAG system will operate abnormally and cannot be automatically recovered in this scenario. To ensure the reliability of peer-link, note the following points when configuring and deploying the peer-link:
  - When configuring the peer link, only the LAG port is supported. In other words, the peer link must always be a LAG port.
  - A minimum of two directly connected physical ports should be used for peer link LAG port. The peer link connecting the two MLAG peer devices should be directly connected meaning that no intermediate transmission devices should be used on the peer link. All of the directly connected physical ports should be added into one LAG port to form the peer-link. We don't support more than one L2 connection between MLAG peer switches meaning that only one peer link is supported between the two peer devices.
  - 10G or 40G speed ports should be used on peer link. It is highly recommended to provide enough bandwidth for the peer link when the network is deployed.
  - Any manual action to shutdown the peer link is strictly forbidden.
  - Any MLAG VLAN and non-MLAG VLAN MUST be allowed on MLAG peer-link.
  - When numerous rapid PVST+ instances are configured, exceeding the default BPDU queue processing rate in CPU will result in BPDU packet loss or network loops. To resolve this problem, you can use CoPP command **set class-of-service scheduler bpdu-scheduler max-bandwidth-pps** <*value*> to increase the maximum bandwidth of BPDU queue. By default, the value is 80pps.
  - When numerous MLAG instances are configured, exceeding the default MLAG queue processing rate in CPU will result in MLAG packet loss. To resolve this problem, you can use the following CoPP command to increase the maximum bandwidth for MLAG and MLAG MAC SYNC queues. By default, the value is 80pps.

    set class-of-service scheduler mlag-scheduler max-bandwidth-pps <*value*>

    set class-of-service scheduler mlag-mac-sync-scheduler max-bandwidth-pps <value>
- Please proceed with caution when removing the peer-link interface from a VLAN, it may cause problems in spanning tree calculation if proper attention is not paid to its potential ramifications.
- MLAG supports to deploy with IGMP snooping.
- MLAG supports to deploy with DHCP snooping.
- MLAG supports to deploy with DHCP relay.
- MLAG supports to deploy with rapid PVST+ or MSTP.
- MLAG supports to deploy with VXLAN.
- If an L3 device is dual-home attached to the MLAG domain as a leaf node, ECMP should be configured on the uplink ports of the leaf node instead of LAG.
- When deploying VRRP in MLAG topology, pay attention to following points:
  - A pair of MLAG ports should be added into one VRRP instance. Multiple pairs within the same VLAN can be added into one VRRP instance as well. However, MLAG ports with different VLANs should be added into different VRRP instances.
  - Active-active VRRP should be used in order to support load-balancing between the two links connected to the Access Layer device.
- After the configuration is changed from inconsistent to consistent, you need to restart the MLAG peer devices to ensure that MLAG functions normally.

Configuring MLAG

MLAG configuration process is in the following steps:

1. Configure the VLAN and the VLAN interface.
2. Configure LAG interface and add ports to the LAG.
3. Ping peer IP to verify L3 connection is ok on peer link.
4. Configure the MLAG domain, MLAG node and peer link.
5. Show MLAG domain and configuration consistency to verify MLAG session status is ok.
6. Configure link ID on the MLAG member port.
7. Show MLAG link to verify MLAG port is ok.

Procedure

Step1 Configure the VLAN and the VLAN interface.

a) Configure a VLAN ID.

set vlans vlan-id <*vlan-id*>

b) Configur the L3 VLAN interface.

set vlans vlan-id <*vlan-id*> **l3-interface** <*interface-name*>

c) Configure the L3 interface IP address for peer link port on local MLAG peer device.

set l3-interface vlan-interface <*interface-name*> **address** <ip-*address*> **prefix-length** <*number*>

Step2 Configure LAG interface and add ports to the LAG.

set interface aggregate-ethernet <*lag-interface-name*>

set interface gigabit-ethernet <*port-name*> **ether-options 802.3ad** <*lag-interface-name*>

Step3 Ping peer IP to verify L3 connection is ok on peer link.

Step4 Configure an MLAG domain ID.

set protocols mlag domain <*domain-id*>

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify the node number for each MLAG peer device. One of the MLAG peer devices should be Node 0 and the other is Node 1.

set protocols mlag domain <*domain-id*> **node** <**0 | 1**>

Step6 Configure the peer IP address and peer link port.

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-link** <*peer-interface-name*>

NOTE: Peer-link port should be configured as a LAG port.

Step7 Show the MLAG domain and configuration consistency to verify MLAG session status is ok.

run show mlag domain {<*domain-id*>| **summary**}

run show mlag consistency-parameter { **link** <link-id>| **summary**}

Step8 Configure link ID on the MLAG member port.

set protocols mlag domain <*domain-id*> **interface** <*lag-interface*> **link** <*link-id*>

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-vlan** <*vlan-id*>

Step10 Show the MLAG link to verify MLAG port is ok.

run show mlag link {<*link-id*>| **summary**}

Configuration Example of MLAG

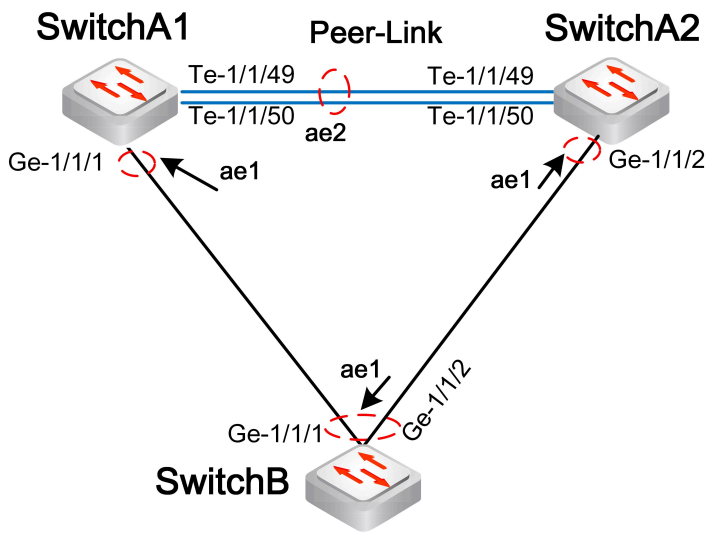
- Example for Configuring a Basic MLAG
- Example for Configuring MLAG with Active-Active-VRRP
- Example for Configuring MLAG with DHCP Relay
- Example for Configuring MLAG with DHCP Snooping
- Example for Configuring MLAG with IGMP Snooping
- Example for Configuring MLAG with Rapid PVST+
- Example for Configuring MLAG with VXLAN

Example for Configuring a Basic MLAG

- Networking Requirements
- Procedure
  - SwitchA1
  - SwitchA2
  - SwitchB
- Verify the Configuration

Networking Requirements

Figure 1 Basic MLAG Topology



In **Figure 1**, SwitchB dual accesses the network through SwitchA1 and SwitchA2 using LACP LAG.

At first, SwitchB accesses the network through SwitchA1. If SwitchA1 or the link between SwitchB and SwitchA1 fails, SwitchB cannot communicate with the network. To avoid service interruptions, we can configure MLAG on SwitchA1 and SwitchA2. When communication between SwitchB and SwitchA1 fails, traffic from the SwitchB will be switched to SwitchA2 seamlessly. When SwitchA1 or the link between SwitchB and SwitchA1 recovers, traffic from the SwitchB will be switched back to SwitchA1.

The peer link between SwitchA1 and SwitchA2 is configured to carry MLAG related control traffic and is very critical to the operation of MLAG function.

Procedure

SwitchA1

Step1 Configure the VLANs.

```
admin@SwitchA1# set vlans vlan-id 15
admin@SwitchA1# set vlans vlan-id 16
admin@SwitchA1# set vlans vlan-id 4088 l3-interface vlan4088
admin@SwitchA1# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@SwitchA1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15
admin@SwitchA1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16
admin@SwitchA1# set interface aggregate-ethernet ae2 family ethernet-switching native-vlan-id 4088
admin@SwitchA1# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@SwitchA1# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15
admin@SwitchA1# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16
```

Step2 Configure MLAG interfaces with LACP mode.

```
admin@SwitchA1# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step3 Add member interfaces to a LAG.

```
admin@SwitchA1# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@SwitchA1# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae2
admin@SwitchA1# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae2
```

Step4 Configure an MLAG domain ID.

admin@SwitchA1# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify SwitchA1 as MLAG Node 0.

admin@SwitchA1# set protocols mlag domain 10 node 0

Step6 Configure the peer IP address and peer link port.

admin@SwitchA1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-link ae2

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@SwitchA1# set l3-interface vlan-interface vlan4088 address 10.10.0.1 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@SwitchA1# set protocols mlag domain 10 interface ae1 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@SwitchA1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-vlan 4088

Step10 Commit the configuration.

admin@SwitchA1# commit

SwitchA2

The configuration on SwitchA2 is the same as SwitchA1.

Step1 Configure the VLANs.

admin@SwitchA2# set vlans vlan-id 15

admin@SwitchA2# set vlans vlan-id 16

admin@SwitchA2# set vlans vlan-id 4088 l3-interface vlan4088

admin@SwitchA2# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@SwitchA2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15

admin@SwitchA2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

admin@SwitchA2# set interface aggregate-ethernet ae2 family ethernet-switching native-vlan-id 4088

admin@SwitchA2# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@SwitchA2# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15

admin@SwitchA2# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16

Step2 Configure MLAG interfaces with LACP mode.

admin@SwitchA2# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

Step3 Add member interfaces to a LAG.

admin@SwitchA2# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@SwitchA2# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae2

admin@SwitchA2# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae2

Step4 Configure an MLAG domain ID.

admin@SwitchA2# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify SwitchA2 as MLAG Node 1.

admin@SwitchA2# set protocols mlag domain 10 node 1

Step6 Configure the peer IP address and peer link port.

admin@SwitchA2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-link ae2

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@SwitchA2# set l3-interface vlan-interface vlan4088 address 10.10.0.2 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@SwitchA2# set protocols mlag domain 10 interface ae1 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@SwitchA2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-vlan 4088

Step10 Commit the configuration.

admin@SwitchA2# commit

SwitchB

Step1 Enable aggregation interface with LACP mode.

admin@SwitchB# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

Step2 Add member interfaces to a LAG.

admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1

Step3 Configure VLAN.

admin@SwitchB# set vlans vlan-id 15

admin@SwitchB# set vlans vlan-id 16

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

Step4 Commit the configuration.

admin@SwitchB# commit

Verify the Configuration

- You can use the **run show mlag domain** command to display the global MLAG domain information.

```
admin@SwitchA1# run show mlag domain summary
Domain ID: 10    Domain MAC: 48:6E:73:FF:00:0a    Node ID: 0
-------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status  Config Matched   MAC Synced   # of Links
---------  ---------------  ---------  ---------------  --------------   ----------   ----------
ae2        10.10.10.2       4088       ESTABLISHED       Yes              Yes           1
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@SwitchA1# run show mlag link summary
# of Links: 1
Link   Local LAG   Link Status   Local Status   Peer Status    Config Matched   Flood
----   ---------   -----------   ------------   -----------     --------------   -----
2      ae1          IDLE            UP           UNKNOWN        No              No
```

- You can use the **run show mlag consistency-parameter** command to display the result of MLAG configuration consistency check, including the global and per MLAG configuration.

```
admin@SwitchA1# run show mlag consistency-parameter link 2
Port Configurations:
-----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
MTU                     1514             1514             PASS
Mac Learning            Yes              Yes              PASS
Lag Mode                LACP             LACP             PASS
Native Vlan             1                1                PASS
Port Vlan Mode          Trunk            Trunk            PASS
Trunk Vlan Count        2                2                PASS
Trunk VLAN IDs                                            PASS

Spanning-Tree Configurations:
-----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Mode                                                      PASS

VXLAN Configurations:
-----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Link   1 VXLAN          N/A              N/A              FAIL

admin@SwitchA1# run show mlag consistency-parameter summary
Overall : PASS
--------------
```

```
Global  : PASS
Link 2  : PASS

MLAG Configurations:
------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Domain ID                1                1                PASS
Node ID                  0                1                PASS
Peer VLAN                4088             4088             PASS
Link Count               1                1                PASS
Link IDs                 2                2                PASS

Spanning-Tree Configurations:
------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS

DHCP Snooping Configurations:
------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
VLAN Count               0                4                FAIL
VLAN IDs                                                   FAIL

IGMP Snooping Configurations:
------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS

VXLAN Configurations:
------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
VXLAN                    N/A              N/A              PASS
VXLAN VNI Count          0                0                PASS
VXLAN VNIs                                                 PASS
```

- You can use the **run show lacp neighbor** command to view the config information of LACP neighbor.

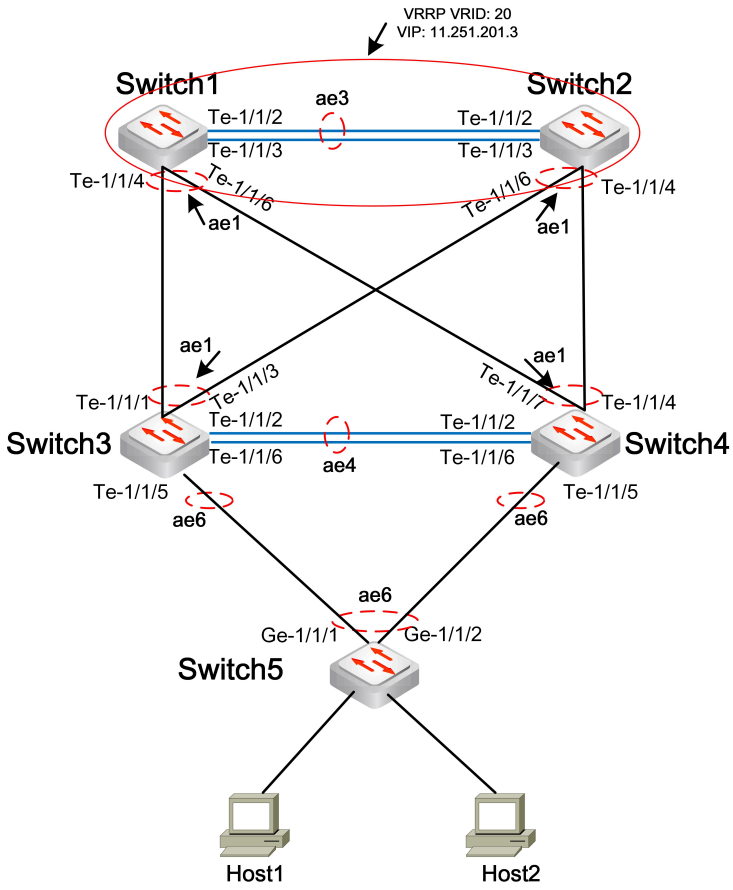
```
admin@SwitchA1# run show lacp neighbor
     Aggregated interface: ae1
     Port Number   Partner System ID               Partner Port Num   Port Priority   Admin Key   Oper Key   State
     -----------          ----------------------   ----------------   -------------    ---------  --------   -----
      ge-1/1/1         32768,08:9E:01:61:64:13       1                 32768            0x00       0x35        0x3
      Aggregated interface: ae2
      Port Number   Partner System ID                    Partner Port Num   Port Priority   Admin Key   Oper Key
      ------------------------------------------------------------------------------------------------------------
       te-1/1/49           32768,70:72:CF:B7:60:A5 73       73                  32768           0x00       0x50
       te-1/1/50           32768,70:72:CF:B7:60:A5 73       74                  32768           0x00       0x50
```

Example for Configuring MLAG with Active-Active-VRRP

- Networking Requirements
  - Basic Deployment
  - Networking Address Planning
- Procedure
  - Switch1
  - Switch2
  - Switch3
  - Switch4
  - Switch5
- Verify the Configuration

Networking Requirements

Figure 1. User Configuration Topology of MLAG with VRRP



When an MLAG is configured to provide L3 routing functions to downstream clients, the MLAG peers should provide the same gateway address to the downstream clients. VRRP groups combine the MLAG peer devices into a virtual router and use the IP address of the VRRP virtual router to communicate with the access devices as the default gateway address. When one device in the VRRP group fails, VRRP mechanism can elect a new gateway to transmit service traffic thus ensuring the reliable operation of the layer-3 network.

Basic Deployment

- In **Figure 1**, a two-layer MLAG is deployed in the topology, where Switch1 and Switch2 form an MLAG peer at aggregation layer, Switch3 and Switch4 form an MLAG peer at access layer. Switch1and Switch2 are in MLAG domain 1; Switch3 and Switch4 are in MLAG domain 2. It is mandatory that different pairs of MLAG peer devices should use different domain IDs.
- In the two-layer MLAG topology, MLAG member ports on the MLAG peer in the same domain MUST belong to the same MLAG, that is, the member ports should be configured with the same link ID. Use link ID 1 on Switch1 and Switch2 to bind all the MLAG member ports, link ID 2 is used on Switch3 and Switch4.
- Active-Active VRRP is deployed on Switch1 and Switch2 as Gateway for Host devices of VLAN 20.
- Access Switch5 dual-accesses to the network through Switch3 and Switch4 by LAG interface.

Networking Address Planning

The networking IP address planning is shown in the following table.

Switch	Physical Interface	Aggregate Interface	VLAN Interface and IP Address
Switch1	Te-1/1/2	ae3	VLAN interface 4092: 192.168.45.2
	Te-1/1/3		
	Te-1/1/4	ae1	VLAN interface 20: 11.251.201.1
	Te-1/1/6		VRRP virtual IP: 11.251.201.3
Switch2	Te-1/1/2	ae3	VLAN interface 4092: 192.168.45.1
	Te-1/1/3		
	Te-1/1/4	ae1	VLAN interface 20: 11.251.201.2
	Te-1/1/6		VRRP virtual IP: 11.251.201.3
Switch3	Te-1/1/2	ae4	VLAN interface 4093: 192.168.46.2
	Te-1/1/6		
	Te-1/1/1	ae1	-
	Te-1/1/3		
	Te-1/1/5	ae6	-
Switch4	Te-1/1/2	ae4	VLAN interface 4093: 192.168.46.1
	Te-1/1/6		
	Te-1/1/4	ae1	-
	Te-1/1/7		
	Te-1/1/5	ae6	-
Switch5	Ge-1/1/1	ae6	-
	Ge-1/1/2		

Procedure

Switch1

Step1 Configure the aggregation interface with LACP mode.

```
admin@Switch1# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step2 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 10-19
admin@Switch1# set vlans vlan-id 20 l3-interface 20
admin@Switch1# set vlans vlan-id 4088 l3-interface 4088
admin@Switch1# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 10
admin@Switch1# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10-19
admin@Switch1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Switch1# set interface aggregate-ethernet ae3 family ethernet-switching native-vlan-id 4088
admin@Switch1# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 10-19
admin@Switch1# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 20
```

Step3 Configure the L3 interface IP address.

```
admin@Switch1# set l3-interface vlan-interface 4088 address 192.168.45.2 prefix-length 24
admin@Switch1# set l3-interface vlan-interface 20 address 11.251.201.1 prefix-length 24
```

Step4 Add interfaces to the LAG port.

```
admin@Switch1# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae3
admin@Switch1# set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad ae3
admin@Switch1# set interface gigabit-ethernet te-1/1/4 ether-options 802.3ad ae1
admin@Switch1# set interface gigabit-ethernet te-1/1/6 ether-options 802.3ad ae1
```

Step5 Configure MLAG domain ID.

```
admin@Switch1# set protocols mlag domain 1
```

Step6 Specify Switch1 as Node 0 of MLAG domain 1.

```
admin@Switch1# set protocols mlag domain 1 node 0
```

Step7 Configure link ID on the MLAG member port.

```
admin@Switch1# set protocols mlag domain 1 interface ae1 link 1
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step8 Configure the peer IP address and the peer-link for the MLAG peer.

```
admin@Switch1# set protocols mlag domain 1 peer-ip 192.168.45.1 peer-link ae3
```

Step9 Configure MLAG peer VLAN.

```
admin@Switch1# set protocols mlag domain 1 peer-ip 192.168.45.1 peer-vlan 4088
```

Step10 Enable Active-Active-VRRP function.

```
admin@Switch1# set protocols vrrp interface 20 vrid 20 ip 11.251.201.3
admin@Switch1# set protocols vrrp interface 20 vrid 20 load-balance disable false
```

Step11 Commit the configuration.

```
admin@Switch1# commit
```

Switch2

Step1 Configure the aggregation interface with LACP mode.

```
admin@Switch2# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step2 Configure the VLANs.

```
admin@Switch2# set vlans vlan-id 10-19
admin@Switch2# set vlans vlan-id 20 l3-interface 20
admin@Switch2# set vlans vlan-id 4088 l3-interface 4088
admin@Switch2# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 10
admin@Switch2# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Switch2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10-19
admin@Switch2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Switch2# set interface aggregate-ethernet ae3 family ethernet-switching native-vlan-id 4088
admin@Switch2# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk
admin@Switch2# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 10-19
admin@Switch2# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 20
```

Step3 Configure the L3 interface IP address.

```
admin@Switch2# set l3-interface vlan-interface 4088 address 192.168.45.1 prefix-length 24
admin@Switch2# set l3-interface vlan-interface 20 address 11.251.201.1 prefix-length 24
```

Step4 Add interfaces to the LAG port.

```
admin@Switch2# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae3
admin@Switch2# set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad ae3
admin@Switch2# set interface gigabit-ethernet te-1/1/4 ether-options 802.3ad ae1
admin@Switch2# set interface gigabit-ethernet te-1/1/6 ether-options 802.3ad ae1
```

Step5 Configure MLAG domain ID.

```
admin@Switch2# set protocols mlag domain 1
```

Step6 Specify Switch2 as Node 1 of MLAG domain 1.

```
admin@Switch2# set protocols mlag domain 1 node 1
```

Step7 Configure link ID on the MLAG member port.

```
admin@Switch2# set protocols mlag domain 1 interface ae1 link 1
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step8 Configure the peer IP address and the peer-link for the MLAG peer.

```
admin@Switch2# set protocols mlag domain 1 peer-ip 192.168.45.2 peer-link ae3
```

Step9 Configure MLAG peer VLAN.

```
admin@Switch2# set protocols mlag domain 1 peer-ip 192.168.45.2 peer-vlan 4088
```

Step10 Enable Active-Active-VRRP function.

```
admin@Switch2# set protocols vrrp interface 20 vrid 20 ip 11.251.201.3
admin@Switch2# set protocols vrrp interface 20 vrid 20 load-balance disable false
```

Step11 Commit the configuration.

```
admin@Switch2# commit
```

Switch3

Step1 Configure the aggregation interfaces with LACP mode.

```
admin@Switch3# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Switch3# set interface aggregate-ethernet ae6 aggregated-ether-options lacp enable true
```

Step2 Configure the VLANs.

```
admin@Switch3# set vlans vlan-id 10-20
admin@Switch3# set vlans vlan-id 4088 l3-interface 4088
admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 10
admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10-20
admin@Switch3# set interface aggregate-ethernet ae4 family ethernet-switching native-vlan-id 4088
admin@Switch3# set interface aggregate-ethernet ae4 family ethernet-switching port-mode trunk
admin@Switch3# set interface aggregate-ethernet ae4 family ethernet-switching vlan members 10-20
admin@Switch3# set interface aggregate-ethernet ae6 family ethernet-switching native-vlan-id 10
admin@Switch3# set interface aggregate-ethernet ae6 family ethernet-switching port-mode trunk
admin@Switch3# set interface aggregate-ethernet ae6 family ethernet-switching vlan members 10-20
```

Step3 Configure the L3 interface IP address.

```
admin@Switch3# set l3-interface vlan-interface 4088 address 192.168.46.2 prefix-length 24
```

Step4 Configure MLAG domain ID.

```
admin@Switch3# set protocols mlag domain 2
```

Step5 Specify Switch3 as Node 0 of MLAG domain 2.

```
admin@Switch3# set protocols mlag domain 2 node 0
```

Step6 Configure link ID on the MLAG member port.

```
admin@Switch3# set protocols mlag domain 2 interface ae1 link 2
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step7 Add member interfaces to the LAG ports.

```
admin@Switch3# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae4
admin@Switch3# set interface gigabit-ethernet te-1/1/6 ether-options 802.3ad ae4
admin@Switch3# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae1
admin@Switch3# set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad ae1
admin@Switch3# set interface gigabit-ethernet te-1/1/5 ether-options 802.3ad ae6
```

Step8 Configure the peer IP address and the peer-link for the MLAG peer.

```
admin@Switch3# set protocols mlag domain 2 peer-ip 192.168.46.1 peer-link ae4
```

Step9 Configure MLAG peer VLAN.

```
admin@Switch3# set protocols mlag domain 2 peer-ip 192.168.46.1 peer-vlan 4088
```

Step10 Commit the configuration.

```
admin@Switch3# commit
```

Switch4

Step1 Configure the aggregation interfaces with LACP mode.

```
admin@Switch4# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Switch4# set interface aggregate-ethernet ae6 aggregated-ether-options lacp enable true
```

Step2 Configure the VLANs.

```
admin@Switch4# set vlans vlan-id 10-20
admin@Switch4# set vlans vlan-id 4088 l3-interface 4088
admin@Switch4# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 10
admin@Switch4# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Switch4# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10-20
admin@Switch4# set interface aggregate-ethernet ae4 family ethernet-switching native-vlan-id 4088
admin@Switch4# set interface aggregate-ethernet ae4 family ethernet-switching port-mode trunk
admin@Switch4# set interface aggregate-ethernet ae4 family ethernet-switching vlan members 10-20
admin@Switch4# set interface aggregate-ethernet ae6 family ethernet-switching native-vlan-id 10
admin@Switch4# set interface aggregate-ethernet ae6 family ethernet-switching port-mode trunk
admin@Switch4# set interface aggregate-ethernet ae6 family ethernet-switching vlan members 10-20
```

Step3 Configure the L3 interface IP address.

```
admin@Switch4# set l3-interface vlan-interface 4088 address 192.168.46.1 prefix-length 24
```

Step4 Configure MLAG domain ID.

```
admin@Switch4# set protocols mlag domain 2
```

Step5 Specify Switch4 as Node 1 of MLAG domain 2.

```
admin@Switch4# set protocols mlag domain 2 node 1
```

Step6 Configure link ID on the MLAG member port.

```
admin@Switch4# set protocols mlag domain 2 interface ae1 link 2
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step7 Add member interfaces to the LAG ports.

```
admin@Switch4# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae4
admin@Switch4# set interface gigabit-ethernet te-1/1/6 ether-options 802.3ad ae4
admin@Switch4# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae1
admin@Switch4# set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad ae1
admin@Switch4# set interface gigabit-ethernet te-1/1/5 ether-options 802.3ad ae6
```

Step8 Configure the peer IP address and the peer-link for the MLAG peer.

```
admin@Switch4# set protocols mlag domain 2 peer-ip 192.168.46.2 peer-link ae4
```

Step9 Configure MLAG peer VLAN.

```
admin@Switch4# set protocols mlag domain 2 peer-ip 192.168.46.2 peer-vlan 4088
```

Step10 Commit the configuration.

```
admin@Switch4# commit
```

Switch5

Step1 Enable the aggregation interface with LACP mode.

```
admin@Switch5# set interface aggregate-ethernet ae6 aggregated-ether-options lacp enable true
```

Step2 Add the interfaces to the LAG ports.

```
admin@Switch5# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae6
admin@Switch5# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae6
```

Step3 Configure the VLANs.

```
admin@Switch5# set vlans vlan-id 10-20
admin@Switch5# set interface aggregate-ethernet ae6 family ethernet-switching native-vlan-id 10
admin@Switch5# set interface aggregate-ethernet ae6 family ethernet-switching port-mode trunk
admin@Switch5# set interface aggregate-ethernet ae6 family ethernet-switching vlan members 10-20
```

Verify the Configuration

- You can use the **run show mlag domain** command to display the global MLAG domain information.

```
admin@Switch1# run show mlag domain summary
Domain ID: 1 Domain MAC: 48:6E:73:FF:00:01 Node ID: 0
------------------------------------------------------------------------
Peer Link Peer IP         Peer Vlan Neighbor Status Config Matched MAC Synced # of Links
--------- --------------- --------- --------------- -------------- ---------- ----------
ae3       10.10.10.2      4088      ESTABLISHED      Yes            Yes        1
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@Switch1# run show mlag link summary
# of Links: 1
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
```

- You can use the **run show mlag consistency-parameter** command to display the result of MLAG configuration consistency check, including the global and per MLAG configuration.

```
admin@Switch1# run show mlag consistency-parameter link 1
Port Configurations:
------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
MTU                     1514             1514             PASS
Mac Learning            Yes              Yes              PASS
Lag Mode                LACP             LACP             PASS
Native Vlan             1                1                PASS
Port Vlan Mode          Trunk           Trunk             PASS

Spanning-Tree Configurations:
------------------------------------------------------------------
Property                Local Value      Peer Value       Result
```

```
----------------------  ---------------  ---------------  ------
Mode                                                      PASS

admin@Switch1# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS


MLAG Configurations:
-------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Domain ID               1                1                PASS
Node ID                 0                1                PASS
Peer VLAN               4088             4088             PASS
Link Count              1                1                PASS
Link IDs                2                2                PASS

Spanning-Tree Configurations:
-------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS

DHCP Snooping Configurations:
-------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS

IGMP Snooping Configurations:
-------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS
```

- You can use **run show vrrp** command to view the configuration information of VRRP group. The result of show command on Switch1 is as follows.

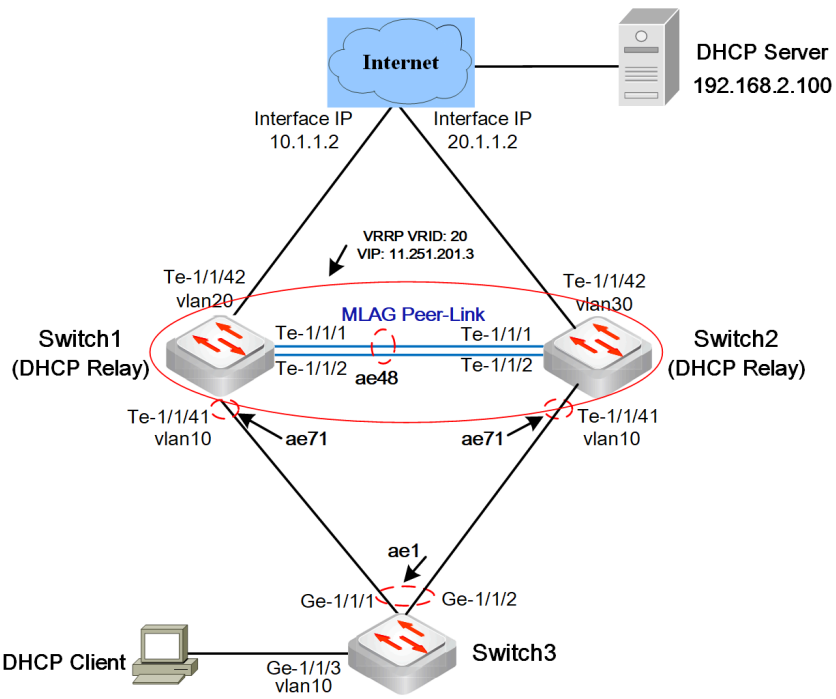
```
admin@Switch1# run show vrrp
Interface:                    20
VRID:                         20
Version:                      2
Load-balance:                 enable
State:                        Master
Master IP:                    11.251.201.1
Virtual MAC:                  00:00:5e:00:01:01
Preempt:                      enable
Adver Interval:               4
Priority:                     100
Virtual IP:                   11.251.201.3
Auth-type:                    none
Auth-key:
```

Example for Configuring MLAG with DHCP Relay

- Networking Requirements
- Procedure
  - Switch1
    - MLAG Configuration
    - VRRP Configuration
    - DHCP Relay Configuration
    - Other Configuration
  - Switch2
    - MLAG Configuration
    - VRRP Configuration
    - DHCP Relay Configuration
    - Other Configuration
  - Switch3
  - Verify the Configuration

Networking Requirements

Figure 1. Example for Configuring MLAG with DHCP Relay



As shown in **Figure 1**, Switch 1 and Switch 2 are a pair of MLAG peers. DHCP client connects to Switch 3 which is dual-homed to the MLAG network. The DHCP client in network segment 10.20.20.0/24 wants to dynamically obtain IP address from the DHCP server which is in a different subnet. In this case, we need to configure DHCP relay on MLAG peers to forward DHCP packets between client and server.

When an MLAG is deployed to provide L3 routing functions to downstream clients, the MLAG peers should provide the same gateway address to the downstream clients. VRRP groups combine the MLAG peer devices into a virtual router and use the IP address of the VRRP virtual router to communicate with the access devices as the default gateway address.

Follow the configuration roadmap below to complete the example for configuring MLAG with DHCP relay:

1. Configure Switch 1 and Switch 2 as an MLAG pair.
2. Configure Active-Active VRRP on Switch1 and Switch2 as a virtual Gateway for DHCP client.
3. Enable DHCP relay on Switch 1 and Switch 2.
   - DHCP relay configuration should be identical on both MLAG peer devices.
   - Configure DHCP relay agent IP address to use VRRP virtual IP.
4. Configure a route to DHCP server on Switch 1 and Switch 2. The static route is used as an example.
5. As a Layer 2 device, access Switch3 dual-accesses to the network through Switch1 and Switch2 by a LAG interface.
6. Configure the DHCP client with a gateway address that is the IP address of the VRRP virtual router.

Procedure

Switch1

MLAG Configuration

Step1 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 10
admin@Switch1# set vlans vlan-id 4088 l3-interface vlan4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10
```

Step2 Configure aggregation interfaces with LACP mode.

```
admin@Switch1# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true
admin@Switch1# set interface aggregate-ethernet ae48 aggregated-ether-options lacp enable true
```

Step3 Add member interfaces to the LAG.

```
admin@Switch1# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48
admin@Switch1# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48
admin@Switch1# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71
```

Step4 Configure an MLAG domain ID.

```
admin@Switch1# set protocols mlag domain 10
```

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify Switch1 as MLAG Node 0.

```
admin@Switch1# set protocols mlag domain 10 node 0
```

Step6 Configure the L3 interface IP address for peer link port on local MLAG peer device.

```
admin@Switch1# set l3-interface vlan-interface vlan4088 address 10.10.0.1 prefix-length 24
```

Step7 Configure link ID for the MLAG member port.

```
admin@Switch1# set protocols mlag domain 10 interface ae71 link 1
```

NOTE: The paired MLAG member ports separately configured on two MLAG peer must be bound to the same MLAG link ID.

Step8 Configure MLAG peer link and peer VLAN.

```
admin@Switch1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-link ae48
admin@Switch1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-vlan 4088
```

NOTE: Peer-link port should be configured as a LAG port.

VRRP Configuration

Step 1 Configure the L3 interface IP address.

```
admin@Switch1# set l3-interface vlan-interface vlan10 address 11.251.201.1 prefix-length 24
```

Step 2 Enable Active-Active-VRRP function.

```
admin@Switch1# set protocols vrrp interface vlan10 vrid 100 ip 11.251.201.3
admin@Switch1# set protocols vrrp interface vlan10 vrid 100 load-balance disable false
```

DHCP Relay Configuration

Step 1 Enable IP routing function when using DHCP relay.

```
admin@Switch1# set ip routing enable true
```

Step 2 Enable the DHCP relay function on L3 VLAN interface vlan10.

```
admin@Switch1# set protocols dhcp relay interface vlan10 disable false
```

Step 3 Configure the IP address of DHCP server 192.168.2.100.

```
admin@Switch1# set protocols dhcp relay interface vlan10 dhcp-server-address 192.168.2.100
```

Step 4 Configure DHCP relay agent IP address to use VRRP virtual IP.

```
admin@Switch1# set protocols dhcp relay interface vlan10 relay-agent-address 11.251.201.3
```

Other Configuration

Step1 Configure VLAN and VLAN interface.

```
admin@Switch1# set vlans vlan-id 20
admin@Switch1# set vlans vlan-id 20 l3-interface vlan20
admin@Switch1# set interface gigabit-ethernet te-1/1/42 family ethernet-switching native-vlan-id 20
admin@Switch1# set l3-interface vlan-interface vlan20 address 10.1.1.1 prefix-length 24
```

Step 2 Configure route to DHCP server. The following command configures static route as an example.

```
admin@Switch1# set protocols static route 192.168.2.0/24 next-hop 10.1.1.2
```

Step 3 Commit the configuration.

```
admin@Switch1# commit
```

Switch2

MLAG Configuration

Step 1 Configure the VLANs.

```
admin@Switch2# set vlans vlan-id 10
admin@Switch2# set vlans vlan-id 4088 l3-interface vlan4088
admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088
admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk
admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10
admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk
admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10
```

Step 2 Configure aggregation interfaces with LACP mode.

```
admin@Switch2# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true
admin@Switch2# set interface aggregate-ethernet ae48 aggregated-ether-options lacp enable true
```

Step 3 Add member interfaces to the LAG.

```
admin@Switch2# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48
admin@Switch2# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48
admin@Switch2# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71
```

Step 4 Configure an MLAG domain ID.

```
admin@Switch2# set protocols mlag domain 10
```

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step 5 Specify Switch2 as MLAG Node 1.

```
admin@Switch2# set protocols mlag domain 10 node 1
```

Step 6 Configure the L3 interface IP address for peer link port on local MLAG peer device.

```
admin@Switch2# set l3-interface vlan-interface vlan4088 address 10.10.0.2 prefix-length 24
```

Step 7 Configure link ID for the MLAG member port.

```
admin@Switch2# set protocols mlag domain 10 interface ae71 link 1
```

NOTE: The paired MLAG member ports separately configured on two MLAG peer must be bound to the same MLAG link ID.

Step 8 Configure MLAG peer link and peer VLAN.

```
admin@Switch2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-link ae48
admin@Switch2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-vlan 4088
```

NOTE: Peer-link port should be configured as a LAG port.

VRRP Configuration

Step 1 Configure the L3 interface IP address.

```
admin@Switch2# set l3-interface vlan-interface vlan10 address 11.251.201.2 prefix-length 24
```

Step 2 Enable Active-Active-VRRP function.

```
admin@Switch2# set protocols vrrp interface vlan10 vrid 100 ip 11.251.201.3
admin@Switch2# set protocols vrrp interface vlan10 vrid 100 load-balance disable false
```

DHCP Relay Configuration

Step 1 Enable IP routing function when using DHCP relay.

```
admin@Switch2# set ip routing enable true
```

Step 2 Enable the DHCP relay function on L3 VLAN interface vlan10.

```
admin@Switch2# set protocols dhcp relay interface vlan10 disable false
```

Step 3 Configure the IP address of DHCP server 192.168.2.100.

```
admin@Switch2# set protocols dhcp relay interface vlan10 dhcp-server-address 192.168.2.100
```

Step 4 Configure DHCP relay agent IP address to use VRRP virtual IP.

```
admin@Switch2# set protocols dhcp relay interface vlan10 relay-agent-address 11.251.201.3
```

Other Configuration

Step1 Configure VLAN and VLAN interface.

```
admin@Switch2# set vlans vlan-id 30
admin@Switch2# set vlans vlan-id 30 l3-interface vlan30
admin@Switch2# set interface gigabit-ethernet te-1/1/42 family ethernet-switching native-vlan-id 30
admin@Switch2# set l3-interface vlan-interface vlan30 address 20.1.1.1 prefix-length 24
```

Step2 Configure a route to DHCP server. The following command uses the static route as an example.

```
admin@Switch2# set protocols static route 192.168.2.0/24 next-hop 20.1.1.2
```

Step3 Commit the configuration.

```
admin@Switch2# commit
```

Switch3

Step1 Enable aggregation interface with LACP mode.

```
admin@Switch3# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step2 Add member interfaces to a LAG.

```
admin@Switch3# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@Switch3# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1
```

Step3 Configure VLAN.

```
admin@Switch3# set vlans vlan-id 10
admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 10
```

Step4 Commit the configuration.

```
admin@Switch3# commit
```

Verify the Configuration

- You can use the **run show mlag domain** command to display the global MLAG domain information.

```
admin@Switch1# run show mlag domain summary
Domain ID: 10    Domain MAC: 62:9E:73:FF:00:01    Node ID: 0
------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status  Config Matched  MAC Synced   # of Links
---------  ---------------  ---------  ---------------  --------------  ----------   ----------
ae48       10.10.10.2       4088       ESTABLISHED      Yes              Yes          1
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@Switch1# run show mlag link summary
# of Links: 1
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae71         IDLE          UP             UNKNOWN       No               No
```

- You can use the **run show mlag consistency-parameter** command to display the result of MLAG configuration consistency check, including the global and per MLAG configuration.

```
admin@Switch1# run show mlag consistency-parameter link 1
Port Configurations:
------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
MTU                     1514             1514             PASS
Mac Learning            Yes              Yes              PASS
Lag Mode                LACP             LACP             PASS
Native Vlan             1                1                PASS
Port Vlan Mode          Trunk            Trunk            PASS

Spanning-Tree Configurations:
------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Mode                                                      PASS

admin@Switch1# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS

MLAG Configurations:
------------------------------------------------------------------
Property                Local Value      Peer Value       Result
```

```
----------------------  ---------------  ---------------  ------
Domain ID               1                1                PASS
Node ID                 0                1                PASS
Peer VLAN               4088             4088             PASS
Link Count              1                1                PASS
Link IDs                2                2                PASS

Spanning-Tree Configurations:
--------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS

DHCP Snooping Configurations:
--------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS

IGMP Snooping Configurations:
--------------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                  No               No               PASS
```

- You can use **run show vrrp** command to view the configuration information of VRRP group. The result of show command on Switch1 is as follows.

```
admin@Switch1# run show vrrp
Interface: vlan10
VRID: 100
Version: 2
Load-balance: enable
State: Master
Master IP: 11.251.201.1
Virtual MAC: 00:00:5e:00:01:01
Preempt: disable
Adver Interval: 1
Priority: 250
Virtual IP: 11.251.201.3
Auth-type: none
Auth-key:
```

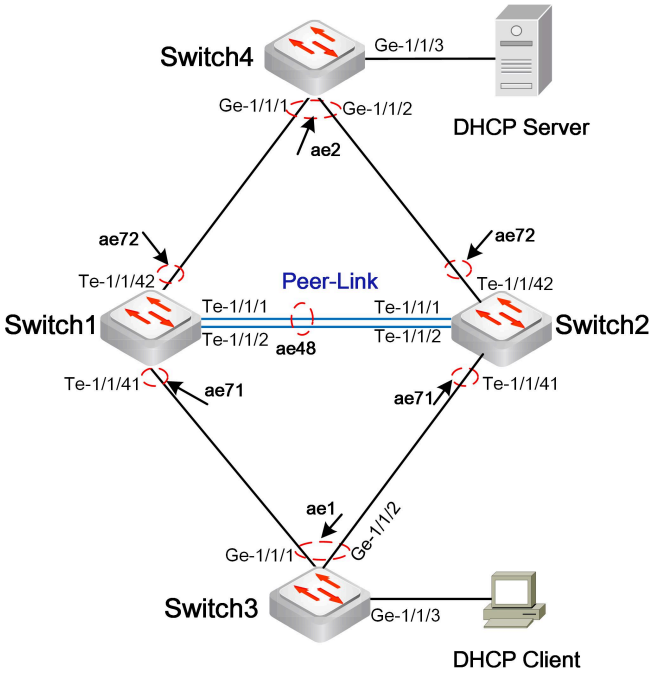
- DHCP client can obtain the IP address normally.

Example for Configuring MLAG with DHCP Snooping

- Networking Requirements
- Procedure
  - Switch1
  - Switch2
  - Switch3
  - Switch4
  - Verify the Configuration

Networking Requirements

Figure 1 User Configuration Topology of MLAG with DHCP Snooping



As shown in **Figure 1**, Switch 1 and Switch 2 are Layer 2 switches and form a pair of MLAG peer devices. The DHCP client is connected to Switch3 which is dual-homed to the MLAG network. The DHCP server is connected to Switch4 which is dual-homed to the MLAG network. In the MLAG topology, to provide better services to DHCP client, the network administrator can configure DHCP snooping on Switch1, Switch2, Switch3 and Switch4, to defend against DHCP attacks.

When configuring the network, you need to pay attention to the following points:

- Switch3 is dual-homed to MLAG peer devices Switch 1 and Switch 2, the link ID is 1. Switch 4 is dual-homed to Switch 1 and Switch 2, the link ID is 2.
- DHCP snooping configuration should be identical on both MLAG peer devices.
- The peer link port should be configured as trust port on demand.
- On Switch1, Switch2, Switch3 and Switch4, configure the interfaces in the direction of the DHCP server as DHCP snooping trusted interfaces.

Procedure

Switch1

Step1 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 10
admin@Switch1# set vlans vlan-id 4088 l3-interface vlan4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10
admin@Switch1# set interface aggregate-ethernet ae72 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae72 family ethernet-switching vlan  members 10
```

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch1# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true

admin@Switch1# set interface aggregate-ethernet ae72 aggregated-ether-options lacp enable true

Step3 Add member interfaces to a LAG.

admin@Switch1# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48

admin@Switch1# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48

admin@Switch1# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71

admin@Switch1# set interface gigabit-ethernet te-1/1/42 ether-options 802.3ad ae72

Step4 Configure an MLAG domain ID.

admin@Switch1# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify Switch1 as MLAG Node 0.

admin@Switch1# set protocols mlag domain 10 node 0

Step6 Configure the peer IP address and peer link port.

admin@Switch1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-link ae48

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@Switch1# set l3-interface vlan-interface vlan4088 address 10.10.0.1 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@Switch1# set protocols mlag domain 10 interface ae71 link 1

admin@Switch1# set protocols mlag domain 10 interface ae72 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@Switch1# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-vlan 4088

Step10 Enable DHCP snooping function.

admin@Switch1# set protocols dhcp snooping vlan 10 disable false

Step11 Configure the interface connected to the DHCP server and peer-link port as DHCP snooping trusted interfaces.

admin@Switch1# set protocols dhcp snooping trust-port ae48

admin@Switch1# set protocols dhcp snooping trust-port ae72

Step12 Commit the configuration.

admin@Switch1# commit

Switch2

Step1 Configure the VLANs.

admin@Switch2# set vlans vlan-id 10

admin@Switch2# set vlans vlan-id 4088 l3-interface vlan4088

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10

admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10

admin@Switch2# set interface aggregate-ethernet ae72 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae72 family ethernet-switching vlan members 10

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch2# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true

admin@Switch2# set interface aggregate-ethernet ae72 aggregated-ether-options lacp enable true

Step3 Add member interfaces to a LAG.

admin@Switch2# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48

admin@Switch2# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48

admin@Switch2# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71

admin@Switch2# set interface gigabit-ethernet te-1/1/42 ether-options 802.3ad ae72

Step4 Configure an MLAG domain ID.

admin@Switch2# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify Switch2 as MLAG Node 1.

admin@Switch2# set protocols mlag domain 10 node 1

Step6 Configure the peer IP address and peer link port.

admin@Switch2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-link ae48

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@Switch2# set l3-interface vlan-interface vlan4088 address 10.10.0.2 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@Switch2# set protocols mlag domain 10 interface ae71 link 1

admin@Switch2# set protocols mlag domain 10 interface ae72 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@Switch2# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-vlan 4088

Step10 Enable DHCP snooping function.

admin@Switch2# set protocols dhcp snooping vlan 10 disable false

Step11 Configure the interface connected to the DHCP server and peer-link port as DHCP snooping trusted interfaces.

admin@Switch2# set protocols dhcp snooping trust-port ae48

admin@Switch2# set protocols dhcp snooping trust-port ae72

Step12 Commit the configuration.

admin@Switch2# commit

Switch3

Step1 Configure the VLANs.

admin@Switch3# set vlans vlan-id 10

admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10

admin@Switch3# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 10

admin@Switch3# set interface gigabit-ethernet ge-1/1/3 description "to-client"

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch3# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@Switch3# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1

admin@Switch3# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

Step3 Enable DHCP snooping function.

admin@Switch3# set protocols dhcp snooping vlan 10 disable false

Step4 Configure ae1 as DHCP snooping trusted port.

admin@Switch3# set protocols dhcp snooping trust-port ae1

Step5 Commit the configuration.

admin@Switch3# commit

Switch4

Step1 Configure the VLANs.

admin@Switch4# set vlans vlan-id 10

admin@Switch4# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@Switch4# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 10

admin@Switch4# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 10

admin@Switch4# set interface gigabit-ethernet ge-1/1/3 description "to-server"

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch4# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae2

admin@Switch4# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2

admin@Switch4# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true

Step3 Enable DHCP snooping function.

admin@Switch4# set protocols dhcp snooping vlan 10 disable false

Step4 Configure ge-1/1/3 as DHCP snooping trusted port.

admin@Switch4# set protocols dhcp snooping trust-port ge-1/1/3

Step5 Commit the configuration.

```
admin@Switch4# commit
```

Verify the Configuration

- You can use the **run show mlag domain** command to display the global MLAG domain information.

```
admin@Switch1# run show mlag domain summary
Domain ID: 10    Domain MAC: 48:6E:73:FF:00:0a    Node ID: 0
-------------------------------------------------------------------------
Peer Link  Peer IP  Peer Vlan  Neighbor Status  Config Matched  MAC Synced  # of Links
---------  --------  ------     ---------        --------------  ----------  ----------
ae48      10.10.10.1  4088       ESTABLISHED     Yes              Yes          1
ae48      10.10.10.1  4088       ESTABLISHED     Yes              Yes          2
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@Switch1# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae71         IDLE          UP             UNKNOWN       No               No
2      ae72         IDLE          UP             UNKNOWN       No               No
```

- Run the **run show dhcp snooping** command to view the DHCP snooping binding table.

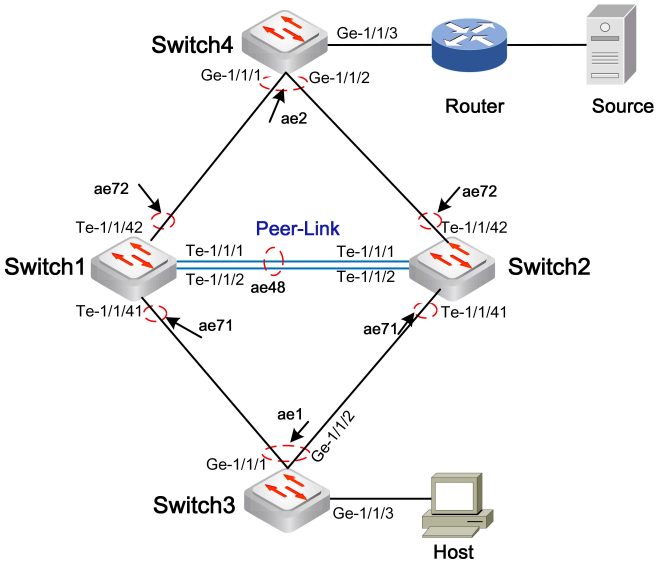
```
admin@Switch3# run show dhcp snooping binding
Total count:     1
MAC Address      IP Address     Port            VLAN ID   Lease(sec)
-----------------------------------------------------------------------------------------------
00:1b:57:60:11:d1   71.0.0.15    ge-1/1/3   10   599/600


admin@Switch4# run show dhcp snooping
Total count:     1
MAC Address         IP Address   Port      VLAN ID      Lease(sec)
-----------------   ---------    --------  -------      ---------------
00:1b:57:60:11:d1   71.0.0.15    ae2        10            599/600
```

Example for Configuring MLAG with IGMP Snooping

- Networking Requirements
- Procedure
  - Switch1
  - Switch2
  - Switch3
  - Switch4
- Verify the Configuration

Networking Requirements

Figure 1 User Configuration Topology of MLAG with IGMP Snooping



As shown in **Figure 1**, a Host connects to a multicast source through the MLAG topology and a Layer 3 Router to receive multicast data from the Source device. Switch3 and Switch4 have dual access to the network through the MLAG peer devices Switch1 and Switch2.

Perform the following procedures on Switch1, Switch2, Switch3 and Switch4 to implement MLAG with IGMP snooping:

- Deploy basic MLAG configurations on Switch1 and Switch2 to form an MLAG topology.
- Enable global and VLAN-based IGMP snooping function on all the switches.

Configuration Notes:

- IGMP snooping configuration should be identical on both MLAG peer devices
- Only the dynamic Layer 2 multicast forwarding entries are synchronized between the MLAG peers, static entries are not synchronized.
- Generally, it is not necessary to configure mrouter port on the peer link.

Procedure

Switch1

Step1 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 10
admin@Switch1# set vlans vlan-id 4088 l3-interface vlan4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10
admin@Switch1# set interface aggregate-ethernet ae72 family ethernet-switching port-mode trunk
admin@Switch1# set interface aggregate-ethernet ae72 family ethernet-switching vlan members 10
```

Step2 Configure aggregation interfaces with LACP mode.

```
admin@Switch1# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true
admin@Switch1# set interface aggregate-ethernet ae72 aggregated-ether-options lacp enable true
```

Step3 Add member interfaces to a LAG.

admin@Switch1# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48

admin@Switch1# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48

admin@Switch1# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71

admin@Switch1# set interface gigabit-ethernet te-1/1/42 ether-options 802.3ad ae72

Step4 Configure an MLAG domain ID.

admin@Switch1# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify Switch1 as MLAG Node 0.

admin@Switch1# set protocols mlag domain 10 node 0

Step6 Configure the peer IP address and peer link port.

admin@Switch1# set protocols mlag domain 10 peer-ip 1.1.1.201 peer-link ae48

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@Switch1# set l3-interface vlan-interface vlan4088 address 1.1.1.166 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@Switch1# set protocols mlag domain 10 interface ae71 link 11

admin@Switch1# set protocols mlag domain 10 interface ae72 link 12

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@Switch1# set protocols mlag domain 10 peer-ip 1.1.1.201 peer-vlan 4088

Step10 Enable IGMP snooping function.

admin@Switch1# set protocols igmp-snooping enable true

admin@Switch1# set protocols igmp-snooping vlan-id 10 enable true

Step11 Commit the configuration.

admin@Switch1# commit

Switch2

Step1 Configure the VLANs.

admin@Switch2# set vlans vlan-id 10

admin@Switch2# set vlans vlan-id 4088 l3-interface vlan4088

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching native-vlan-id 4088

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae48 family ethernet-switching vlan members 10

admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae71 family ethernet-switching vlan members 10

admin@Switch2# set interface aggregate-ethernet ae72 family ethernet-switching port-mode trunk

admin@Switch2# set interface aggregate-ethernet ae72 family ethernet-switching vlan members 10

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch2# set interface aggregate-ethernet ae71 aggregated-ether-options lacp enable true

admin@Switch2# set interface aggregate-ethernet ae72 aggregated-ether-options lacp enable true

Step3 Add member interfaces to a LAG.

admin@Switch2# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae48

admin@Switch2# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae48

admin@Switch2# set interface gigabit-ethernet te-1/1/41 ether-options 802.3ad ae71

admin@Switch2# set interface gigabit-ethernet te-1/1/42 ether-options 802.3ad ae72

Step4 Configure an MLAG domain ID.

admin@Switch2# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify Switch2 as MLAG Node 1.

admin@Switch2# set protocols mlag domain 10 node 1

Step6 Configure the peer IP address and peer link port.

admin@Switch2# set protocols mlag domain 10 peer-ip 1.1.1.166 peer-link ae48

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 VLAN interface IP address for peer link port on local MLAG peer device.

admin@Switch2# set l3-interface vlan-interface vlan4088 address 1.1.1.201 prefix-length 24

Step8 Configure link ID for the MLAG member port.

admin@Switch2# set protocols mlag domain 10 interface ae71 link 11

admin@Switch2# set protocols mlag domain 10 interface ae72 link 12

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

admin@Switch2# set protocols mlag domain 10 peer-ip 1.1.1.166 peer-vlan 4088

Step10 Enable IGMP snooping function.

admin@Switch2# set protocols igmp-snooping enable true

admin@Switch2# set protocols igmp-snooping vlan-id 10 enable true

Step11 Commit the configuration.

admin@Switch2# commit

Switch3

Step1 Configure the VLANs.

admin@Switch3# set vlans vlan-id 10

admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@Switch3# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 10

admin@Switch3# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 10

admin@Switch3# set interface gigabit-ethernet ge-1/1/3 description "to-host"

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch3# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@Switch3# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1

admin@Switch3# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

Step3 Enable IGMP snooping function.

admin@Switch3# set protocols igmp-snooping enable true

admin@Switch3# set protocols igmp-snooping vlan-id 10 enable true

Step4 Commit the configuration.

admin@Switch3# commit

Switch4

Step1 Configure the VLANs.

admin@Switch4# set vlans vlan-id 10

admin@Switch4# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@Switch4# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 10

admin@Switch4# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 10

admin@Switch4# set interface gigabit-ethernet ge-1/1/3 description "to-server"

Step2 Configure aggregation interfaces with LACP mode.

admin@Switch4# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae2

admin@Switch4# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2

admin@Switch4# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true

Step3 Enable IGMP snooping function.

admin@Switch4# set protocols igmp-snooping enable true

admin@Switch4# set protocols igmp-snooping vlan-id 10 enable true

Step4 Commit the configuration.

admin@Switch4# commit

Verify the Configuration

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@Switch1# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
```

```
11      ae71         FULL         UP             UP            Yes             No
12      ae72         FULL         UP             UP            Yes             No

admin@Switch2# run show mlag link summary
# of Links: 2
------------------------------------------------------------------------------
Link  Local LAG  Link Status  Local Status  Peer Status  Config Matched  Flood
----  ---------  -----------  ------------  -----------  --------------  -----
11    ae71        FULL         UP            UP           Yes              No
12    ae72        FULL         UP            UP           Yes              No
```

- You can use the **run show igmp-snooping groups** command to show the multicast group information.

```
admin@Switch1# run show igmp-snooping groups
Total group count: 1
Vlan      Group               Port List          Type
--------  ------------------  -----------------  ----------------------
10        234.0.0.8            ae71               Dynamic
                               ae72               Mrouter

admin@Switch2# run show igmp-snooping groups
Total group count: 1
Vlan      Group               Port List          Type
--------  ------------------  -----------------  ----------------------
10        234.0.0.8            ae71               Dynamic
                               ae72               Mrouter

admin@Switch3# run show igmp-snooping groups
Total group count: 1
Vlan      Group               Port List          Type
--------  ------------------  -----------------  ----------------------
10        234.0.0.8           ge-1/1/3           Dynamic
                              ae1                Mrouter
admin@Switch4# run show igmp-snooping groups
Total group count: 1
Vlan      Group               Port List          Type
--------  ------------------  -----------------  ----------------------
10        234.0.0.8           ae2                Dynamic
                              ge-1/1/3           Mrouter
```

- You can use the **run show igmp-snooping mrouter** command to show the information about IGMP snooping router port.

```
admin@Switch1# run show igmp-snooping mrouter
Vlan      Ports          Type
--------  -------------  ---------
10         ae2            Dynamic

admin@Switch2# run show igmp-snooping mrouter
Vlan      Ports          Type
--------  -------------  ---------
10        ae2            Dynamic

admin@Switch3# run show igmp-snooping mrouter
Vlan      Ports          Type
--------  -------------  ---------
10        ae1            Dynamic

admin@Switch4# run show igmp-snooping mrouter
Vlan      Ports          Type
--------  -------------  ---------
10        ge-1/1/3       Dynamic
```

Example for Configuring MLAG with Rapid PVST+

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
- Verify the Configuration

Networking Requirements

As shown in **Figure 1**, we have implemented MLAG on Switch A and Switch B, the downstream Switch C and Switch D has dual-access to network through Switch A and Switch B respectively.

Rapid PVST+ is deployed in the network to eliminate loops. Devices running rapid PVST+ exchange rapid PVST+ bridge protocol data units (BPDUs) to discover loops in the network and block some ports to prune the network into a loop-free tree network.

Figure1. Example Topology of MLAG with Rapid PVST+

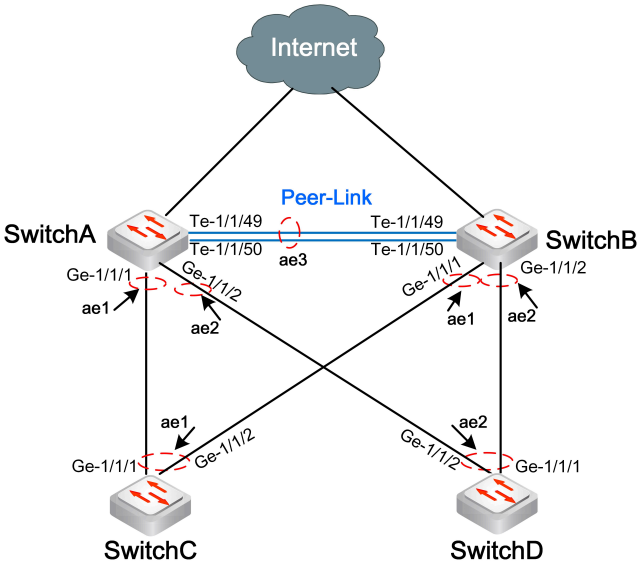


Figure 1 shows the user topology of MLAG with rapid PVST+. Follow the configuration roadmap below to complete the configuration.

- Configure MLAG. Switch A, Switch B and the aggregated port ae1connected to Switch C form an MLAG, link ID is 1; Switch A, Switch B and the aggregated port ae2 connected to Switch D form another MLAG, link ID is 2. MLAG peer-link implements a backup link aggregation group ae3 between Switch A and Switch B to carry MLAG control messages and improve network reliability.
- Configure basic Rapid PVST+ functions to eliminate loops.

Procedure

Configure Switch A, Switch B, Switch C and Switch D according to the networking requirements described above.

Switch A

Step1 Configure the VLANs.

```
admin@SwitchA# set vlans vlan-id 15
admin@SwitchA# set vlans vlan-id 16
admin@SwitchA# set vlans vlan-id 4088 l3-interface 4088
admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15
admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16
admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15
admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16
admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk
admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 4088
admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 15
```

```
admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 16
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 15
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 16
```

Step2 Configure aggregation interfaces with LACP mode.

```
admin@SwitchA# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@SwitchA# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
```

Step3 Add member interfaces to the LAG.

```
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2
admin@SwitchA# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae3
admin@SwitchA# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae3
```

Step4 Configure an MLAG domain ID.

```
admin@SwitchA# set protocols mlag domain 10
```

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify SwitchA as MLAG Node 0.

```
admin@SwitchA# set protocols mlag domain 10 node 0
```

Step6 Configure the peer IP address and peer link port.

```
admin@SwitchA# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-link ae3
```

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

```
admin@SwitchA# set l3-interface vlan-interface 4088 address 10.10.0.1 prefix-length 24
```

Step8 Configure link ID for the MLAG member port.

```
admin@SwitchA# set protocols mlag domain 10 interface ae1 link 1
admin@SwitchA# set protocols mlag domain 10 interface ae2 link 2
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

```
admin@SwitchA# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-vlan 4088
```

Step10 Configure rapid PVST+.

a. Enable spanning tree on Switch A.

```
admin@SwitchA# set protocols spanning-tree enable true
```

By default, spanning tree function is enabled.

b. Configure spanning tree mode in rapid PVST+.

```
admin@SwitchA# set protocols spanning-tree force-version 4
```

c. Enable rapid PVST+ on VLAN instance.

```
admin@SwitchA# set protocols spanning-tree pvst vlan 15 enable true
admin@SwitchA# set protocols spanning-tree pvst vlan 16 enable true
admin@SwitchA# set protocols spanning-tree pvst vlan 4088 enable true
```

Step11 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure the VLANs.

```
admin@SwitchB# set vlans vlan-id 15
admin@SwitchB# set vlans vlan-id 16
admin@SwitchB# set vlans vlan-id 4088 l3-interface 4088
admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching port- mode trunk
admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15
admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16
admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15
admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16
admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk
admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 4088
admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 15
admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 16
admin@SwitchB# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 15
admin@SwitchB# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 16
```

Step2 Configure aggregation interfaces with LACP mode.

```
admin@SwitchB# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@SwitchB# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
```

Step3 Add member interfaces to the LAG.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2
admin@SwitchB# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae3
admin@SwitchB# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae3
```

Step4 Configure an MLAG domain ID.

```
admin@SwitchB# set protocols mlag domain 10
```

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step5 Specify SwitchB as MLAG Node 1.

```
admin@SwitchB# set protocols mlag domain 10 node 1
```

Step6 Configure the peer IP address and peer link port.

```
admin@SwitchB# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-link ae3
```

NOTE: Peer-link port should be configured as a LAG port.

Step7 Configure the L3 interface IP address for peer link port on local MLAG peer device.

```
admin@SwitchB# set l3-interface vlan-interface 4088 address 10.10.0.2 prefix-length 24
```

Step8 Configure link ID for the MLAG member port.

```
admin@SwitchB# set protocols mlag domain 10 interface ae1 link 1
admin@SwitchB# set protocols mlag domain 10 interface ae2 link 2
```

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step9 Configure MLAG peer VLAN.

```
admin@SwitchB# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-vlan 4088
```

Step10 Configure rapid PVST+.

a. Enable spanning tree on Switch B.

```
admin@SwitchB# set protocols spanning-tree enable true
```

By default, spanning tree function is enabled.

b. Configure spanning tree mode in rapid PVST+.

```
admin@SwitchB# set protocols spanning-tree force-version 4
```

c. Enable rapid PVST+ on VLAN instance.

```
admin@SwitchB# set protocols spanning-tree pvst vlan 15 enable true
admin@SwitchB# set protocols spanning-tree pvst vlan 16 enable true
admin@SwitchB# set protocols spanning-tree pvst vlan 4088 enable true
```

Step11 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Enable the aggregation interface with LACP mode.

```
admin@SwitchC# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step2 Add the member interfaces to the LAGs.

```
admin@SwitchC# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1
```

Step3 Configure the VLANs.

```
admin@SwitchC# set vlans vlan-id 15
admin@SwitchC# set vlans vlan-id 16
admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15
admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16
```

Step4 Configure rapid PVST+.

a. Enable spanning tree on Switch C.

```
admin@SwitchC# set protocols spanning-tree enable true
```

By default, spanning tree function is enabled.

b. Configure spanning tree mode in rapid PVST+.

```
admin@SwitchC# set protocols spanning-tree force-version 4
```

c. Enable rapid PVST+ on VLAN instance.

```
admin@SwitchC# set protocols spanning-tree pvst vlan 15 enable true
admin@SwitchC# set protocols spanning-tree pvst vlan 16 enable true
```

Step5 Commit the configuration.

```
admin@SwitchC# commit
```

Switch D

Step1 Enable the aggregation interface with LACP mode.

```
admin@SwitchD# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
```

Step2 Add the member interfaces to the LAG ports.

```
admin@SwitchD# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae2
admin@SwitchD# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2
```

Step3 Configure the VLANs.

```
admin@SwitchD# set vlans vlan-id 15
admin@SwitchD# set vlans vlan-id 16
admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15
admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16
```

Step4 Configure rapid PVST+.

a. Enable spanning tree on Switch D.

```
admin@SwitchD# set protocols spanning-tree enable true
```

By default, spanning tree function is enabled.

b. Configure spanning tree mode in rapid PVST+.

```
admin@SwitchD# set protocols spanning-tree force-version 4
```

c. Enable rapid PVST+ on VLAN instance.

```
admin@SwitchD# set protocols spanning-tree pvst vlan 15 enable true
admin@SwitchD# set protocols spanning-tree pvst vlan 16 enable true
```

Step5 Commit the configuration.

```
admin@SwitchD# commit
```

Verify the Configuration

- You can use the **run show mlag domain** command to check the configuration information of MLAG domain.

  # Check MLAG information on Switch A.

```
admin@SwitchA# run show mlag domain summary
Domain ID: 10    Domain MAC: 48:6E:73:FF:00:0a    Node ID: 0
------------------------------------------------------------------------
Peer Link  Peer IP             Peer Vlan     Neighbor Status  Config Matched   MAC Synced # of Links
---------  ---------------     ---------     ---------------  --------------   ----------   --------------
ae3         10.10.10.2         4088          ESTABLISHED       Yes             Yes          2
```

Check MLAG information on Switch B.

```
admin@SwitchB# run show mlag domain summary
Domain ID: 10    Domain MAC: 48:6E:73:FF:00:0a    Node ID: 1
------------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status  Config Matched   MAC Synced   # of Links
---------  ---------------  ---------  ---------------  --------------  ----------   ----------
ae3        10.10.10.1       4088       ESTABLISHED      Yes              Yes          2
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@SwitchA# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer-Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

- You can use the **run show mlag consistency-parameter** command to display the result of MLAG configuration consistency check, including the global and per MLAG configuration.

```
admin@SwitchA# run show mlag consistency-parameter link 2
Port Configurations:
```

```
-----------------------------------------------------------------
Property           Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
MTU                      1514             1514             PASS
Mac Learning             Yes              Yes              PASS
Lag Mode                 LACP             LACP             PASS
Native Vlan              1                1                PASS
Port Vlan Mode           Trunk           Trunk             PASS

Spanning-Tree Configurations:
-----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Mode                     PVST             PVST             PASS
BPDU Guard               No               No               PASS
Root Guard               No               No               PASS
Manual Forwarding        No               No               PASS
Link Type                P2P              P2P              PASS
Instance Count           1                1                PASS
Instance Vlan 3
-- Port Priority         128              128              PASS
-- Path Cost             0                0                PASS

admin@SwitchA# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS
Link 2  : PASS


MLAG Configurations:
-----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Domain ID                10               10               PASS
Node ID                  0                1                PASS
Peer VLAN                4088             4088             PASS
Link Count               2                 2               PASS
Link IDs                 1  2             1  2             PASS

Spanning-Tree Configurations:
-----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   PVST              PVST            PASS

DHCP Snooping Configurations:
-----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS

IGMP Snooping Configurations:
-----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS
```

Example for Configuring MLAG with VXLAN

- Introduction
- Networking Requirements
- Procedure
  - Configuring MLAG on SwitchA
  - Configuring VXLAN on SwitchA
  - Configuring MLAG on SwitchB
  - Configuring VXLAN on SwitchB
  - Configuring LAG on SwitchC
  - Configuring LAG on SwitchD
- Verifiy the Configuration

Introduction

PICOS-powered Ethernet switches use Multi-Chassis Link Aggregation (MLAG) technology to connect devices, enabling each one to connect to a pair of Pica8 switches with all links running active/active to improve resiliency. There's no need to block certain links, as with the spanning tree protocol (STP), resulting in improved bandwidth utilization and performance. With STP, while redundant links may exist between switches, traffic can only flow over one of them at a time, which effectively cuts the amount of available bandwidth in half. MLAG still supports redundancy, however, because peer switches synchronize forwarding state between them, so if a leaf or spine switch fails, traffic is automatically rerouted for continuous uptime.

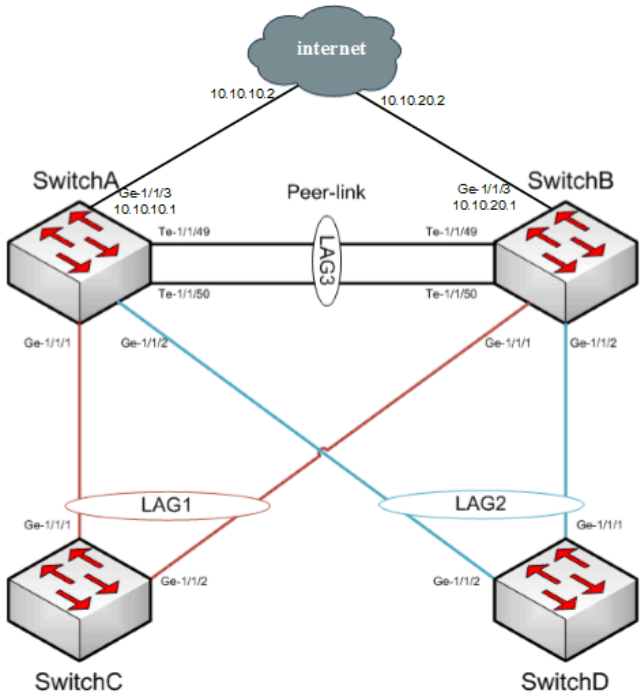
This document describes how to configure MLAG with a Virtual eXtensible LAN (VXLAN), a method for running a Layer 2 overlay network on Layer 3 infrastructure.

Networking Requirements

Figure 1 illustrates an MLAG configured between Switch A and Switch B, the MLAG connections between the neighboring switches, and two downstream Network Devices.

Access Switches SwitchC and SwitchD are dual-homed to an MLAG domain through a VXLAN tunnel, achieving that Layer 2 devices on the access side can communicate with each other over Layer 3 networks.

Figure 1 MLAG Topology with VXLAN



Follow the configuration roadmap below to complete the configuration:

- Configure MLAG. SwitchA, SwitchB and the aggregated port ae1connected to SwitchC form an MLAG, link ID is 1; SwitchA, SwitchB and the aggregated port ae2 connected to SwitchD form another MLAG, link ID is 2. MLAG peer-link implements a backup link aggregation group ae3 between SwitchA and SwitchB to carry MLAG control messages and improve network reliability.
- Configure VXLAN functions on SwitchA and SwitchB.
- Configure LACP LAG ports on Switch C and Switch D to implement dual-homing access.

Procedure

Configuring MLAG on SwitchA

Step1 Configure the aggregation interfaces with LACP mode.

admin@SwitchA# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

admin@SwitchA# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true

Step2 Add member interfaces to a LAG.

admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2

admin@SwitchA# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae3

admin@SwitchA# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae3

Step3 Configure the VLANs.

admin@SwitchA# set vlans vlan-id 15

admin@SwitchA# set vlans vlan-id 16

admin@SwitchA# set vlans vlan-id 4088 l3-interface vlan4088

admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15

admin@SwitchA# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15

admin@SwitchA# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16

admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching native-vlan-id 4088

admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk

admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 15

admin@SwitchA# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 16

Step4 Configure the L3 Interface IP Address.

admin@SwitchA# set l3-interface vlan-interface vlan4088 address 10.10.0.1 prefix-length 24

Step5 Configure MLAG domain ID.

admin@SwitchA# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step6 Specify SwitchA as MLAG Node 0.

admin@SwitchA# set protocols mlag domain 10 node 0

Step7 Configure the peer IP address and peer link port.

admin@SwitchA# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-link ae3

NOTE: Peer-link port should be configured as a LAG port.

Step8 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@SwitchA# set l3-interface vlan-interface vlan4088 address 10.10.0.1 prefix-length 24

Step9 Configure link ID for the MLAG member port.

admin@SwitchA# set protocols mlag domain 10 interface ae1 link 1

admin@SwitchA# set protocols mlag domain 10 interface ae2 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step10 Configure MLAG peer VLAN.

admin@SwitchA# set protocols mlag domain 10 peer-ip 10.10.0.2 peer-vlan 4088

Step11 Commit the configurations.

admin@SwitchA# commit

Configuring VXLAN on SwitchA

Step1 Configure VXLAN soure interface.

admin@SwitchA# set l3-interface loopback lo address 10.10.10.1 prefix-length 32

admin@SwitchA# set vxlans source-interface loopback address 10.10.10.1

Step2 Create VXLAN VNI.

admin@SwitchA# set vxlans vni 100010

Step3 Configure vtep address for VXLAN VNI.

admin@SwitchA# set vxlans vni 100010 flood vtep 20.20.20.1

Step4 Add VXLAN port into VXLAN VNI.

admin@SwitchA# set vxlans vni 100010 vlan 15

Note that, in current version, only one VLAN is supported in one VNI.

Step5 Configure a static route.

admin@SwitchA# set protocols static route 20.20.20.1/24 next-hop 10.10.10.2

Step6 Enable IP routing.

admin@SwitchA# set ip routing enable true

Step7 Commit the configurations.

admin@SwitchA# commit

Configuring MLAG on SwitchB

Step1 Configure the aggregation interfaces with LACP mode.

admin@SwitchB# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

admin@SwitchB# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true

Step2 Add the member interfaces to the LAG ports.

admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2

admin@SwitchB# set interface gigabit-ethernet te-1/1/49 ether-options 802.3ad ae3

admin@SwitchB# set interface gigabit-ethernet te-1/1/50 ether-options 802.3ad ae3

Step3 Configure the VLANs.

admin@SwitchB# set vlans vlan-id 15

admin@SwitchB# set vlans vlan-id 16

admin@SwitchB# set vlans vlan-id 4088 l3-interface vlan4088

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15

admin@SwitchB# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15

admin@SwitchB# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16

admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching native-vlan-id 4088

admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching port-mode trunk

admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 15

admin@SwitchB# set interface aggregate-ethernet ae3 family ethernet-switching vlan members 16

Step4 Configure the L3 Interface IP Address.

admin@SwitchB# set l3-interface vlan-interface vlan4088 address 10.10.0.2 prefix-length 24

Step5 Configure MLAG domain ID.

admin@SwitchB# set protocols mlag domain 10

NOTE: Currently, only one MLAG domain is allowed to be configured on one MLAG device.

Step6 Specify SwitchB as MLAG Node 1.

admin@SwitchB# set protocols mlag domain 10 node 1

Step7 Configure the peer IP address and peer link port.

admin@SwitchB# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-link ae3

NOTE: Peer-link port should be configured as a LAG port.

Step8 Configure the L3 interface IP address for peer link port on local MLAG peer device.

admin@SwitchB# set l3-interface vlan-interface vlan4088 address 10.10.0.2 prefix-length 24

Step9 Configure link ID for the MLAG member port.

admin@SwitchB# set protocols mlag domain 10 interface ae1 link 1

admin@SwitchB# set protocols mlag domain 10 interface ae2 link 2

NOTE: The paired MLAG member ports must be bound to the same MLAG link ID.

Step10 Configure MLAG peer VLAN.

admin@SwitchB# set protocols mlag domain 10 peer-ip 10.10.0.1 peer-vlan 4088

Step11 Commit the configurations.

admin@SwitchB# commit

Configuring VXLAN on SwitchB

Step1 Configure VXLAN soure interface.

admin@SwitchB# set l3-interface loopback lo address 10.10.10.1 prefix-length 32

admin@SwitchB# set vxlans source-interface loopback address 10.10.10.1

Step2 Create VXLAN VNI.

admin@SwitchB# set vxlans vni 100010

Step3 Configure vtep address for VXLAN VNI.

admin@SwitchB# set vxlans vni 100010 flood vtep 20.20.20.1

Step4 Add VXLAN port into VXLAN VNI.

admin@SwitchB# set vxlans vni 100010 vlan 15

Note that, in current version, only one VLAN is supported in one VNI.

Step5 Configure a static route.

admin@SwitchB# set protocols static route 20.20.20.0/24 next-hop 10.10.20.2

Step6 Enable IP routing.

admin@SwitchB# set ip routing enable true

Step7 Commit the configurations.

admin@SwitchB# commit

Configuring LAG on SwitchC

Step1 Configure the aggregation interface with LACP mode.

admin@SwitchC# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true

Step2 Add the member interfaces to the LAG ports.

admin@SwitchC# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1

admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1

Step3 Configure the VLANs.

admin@SwitchC# set vlans vlan-id 15

admin@SwitchC# set vlans vlan-id 16

admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk

admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15

admin@SwitchC# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

Step4 Commit the configurations.

admin@SwitchC# commit

Configuring LAG on SwitchD

Step1 Configure the aggregation interface with LACP mode.

admin@SwitchD# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true

Step2 Add the member interfaces to the LAG ports.

admin@SwitchD# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae2

admin@SwitchD# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae2

Step3 Configure the VLANs.

admin@SwitchD# set vlans vlan-id 15

admin@SwitchD# set vlans vlan-id 16

admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk

admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15

admin@SwitchD# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16

Step4 Commit the configurations.

admin@SwitchD# commit

Verifiy the Configuration

- You can use the **run show vxlan vni** and **run show vxlan tunnel** commands to display the information of VXLAN tunnel.

```
admin@SwitchA# run show vxlan vni 100010
Interface    ID             Type           Egress     Vlan ID
-----------  -----------    -----------    -------    --------
ae1          0x80000001     Access         100078     15
```

```
ae2          0x80000002     Access         100083     15
ge-1/1/3     0x80000005     Network(UC)    100085

admin@SwitchA# run show vxlan tunnel
Total number of tunnels: 1

VNI 100010, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:10.10.10.1, dst addr:20.20.20.1, state:UP
  traffic type:all
  nexthops:10.10.10.2
  output ports:ge-1/1/3
```

- You can use the **run show vxlan address-table** and **run show mac-address table** commands to display the VXLAN MAC address information.

```
admin@SwitchA# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------    ---------------
100010         20:04:0f:0f:49:d1    Dynamic                         20.20.20.1
100010         22:22:22:44:44:44    Dynamic                         20.20.20.1

admin@SwitchB# run show vxlan address-table
VNID           MAC address          Type       Interface          VT EP
-----------    -----------------    -------    ----------------    ---------------
100010         20:04:0f:0f:49:d1    Sync                            10.10.10.1
100010         22:22:22:44:44:44    Sync                            10.10.10.1

admin@SwitchB# run show mac-address table
Total entries in switching table:   3909
Static entries in switching table:  6
Dynamic entries in switching table: 3903

VLAN      MAC address          Type         Age     Interfaces         User
----      -----------------    ---------    ----    ----------------   ----------
15        a0:01:0f:0f:49:f1    Dynamic      300     ae2                xorp
N/A       20:04:0f:0f:49:d1    Peer-Sync    300     vxlan              xorp
N/A       22:22:22:44:44:44    Peer-Sync    300     vxlan              xorp
```

- You can use the **run show mlag domain** command to display the MLAG domain information.

```
admin@SwitchA# run show mlag domain summary
Domain ID: 10    Domain MAC: 48:6E:73:FF:00:0a    Node ID: 0
-------------------------------------------------------------------
Peer Link  Peer IP          Peer Vlan  Neighbor Status  Config Matched   MAC Synced   # of Links
---------  ---------------  ---------  ---------------  --------------  -----------  --------------
ae3        10.10.10.2       4088        ESTABLISHED     Yes              Yes         2
```

- You can use the **run show mlag link** command to display MLAG link information.

```
admin@SwitchA# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer-Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

- After the configuration is complete, the access switches SwitchC and SwitchD can communicate with each other normally.

MLAG Maintenance and Troubleshooting

- How to bind a LAG interface to the MLAG link?
- How to check whether the VLAN configuration on the two peer-link ports are consistent?
- How to confirm whether the MAC address table has been correctly synchronized?
- How to enable MLAG traceoptions
- How to ensure the reliability of the peer link?
- How to verify configurations on MLAG peer are consistent?
- How to verify MLAG link status?
- How to verify MLAG neighbor status?
- How to verify that the peer link connection status is normal?
- How to view and clear MLAG statistics?

How to bind a LAG interface to the MLAG link?

When an MLAG domain is created, you have to associate a pair of MLAG member ports on each MLAG peer device to form an MLAG link by using command **set protocols mlag domain** <*domain-id*> **interface** <*lag-interface*> **link** <*link-id*>.

For example, bind LAG port ae3 to MLAG link 2 of MLAG domain 3.

```
admin@Xorplus# set protocols mlag domain 3 interface ae3 link 2
```

NOTE:

The paired MLAG member ports of the same MLAG must be bound to the same MLAG link ID. Different MLAGs are identified by different link IDs. For example we have two MLAGs in an MLAG Domain then link ID 1 could identify the first MLAG while link ID 2 could identify the second MLAG in the MLAG Domain.

How to check whether the VLAN configuration on the two peer-link ports are consistent?

Any MLAG VLAN and non-MLAG VLAN traffic MUST be allowed on MLAG peer-link. Therefore, the VLAN configurations of the peer-link ports on both ends must be consistent. Run the **run show vlans** command on the MLAG peer devices to check the VLANs of the peer-link port.

For example,

```
admin@PICOS# run show vlans
VlanID  Vlan Name          Tag       Interfaces
------  -----------------  --------  ------------------------------------------------------------
1                          untagged  xe-1/1/1, xe-1/1/2, te-1/1/2, xe-1/1/3, te-1/1/3
                                     xe-1/1/4, te-1/1/4, xe-1/1/5, te-1/1/5, xe-1/1/6
                                     te-1/1/6, te-1/1/7, te-1/1/8, te-1/1/9, te-1/1/10
                                     te-1/1/11, te-1/1/12, te-1/1/13, te-1/1/14, te-1/1/15
                                     te-1/1/16, te-1/1/17, te-1/1/18, te-1/1/19, te-1/1/20
                                     te-1/1/21, te-1/1/22, te-1/1/23, te-1/1/24, te-1/1/25
                                     te-1/1/26, te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30
                                     te-1/1/31, te-1/1/32, te-1/1/33, te-1/1/34, te-1/1/35
                                     te-1/1/36, te-1/1/37, te-1/1/38, te-1/1/39, te-1/1/40
                                     te-1/1/41, te-1/1/42, te-1/1/43, te-1/1/44, te-1/1/45
                                     te-1/1/46, te-1/1/47, te-1/1/48, ae1
                           tagged

2       default            untagged  te-1/1/1
                           tagged    xe-1/1/3

3                          untagged
                           tagged    xe-1/1/3
```

How to confirm whether the MAC address table has been correctly synchronized?

The MLAG peer switches synchronize MAC address table to each other using MAC synchronization message. Only when MLAG neighbor state changes to ESTABLISHED and there is a change in the MAC table, the MAC Sync message will be sent.

To check whether the MAC address tables on both peer devices are consistent, use **run show mac-address table** command to show MAC address table on each MLAG peer device. A MAC address entry contains the VLAN ID, destination MAC address, entry type, aging time and outbound interface.

For details about how MAC tables are synchronized between the MLAG peer devices, see section **MAC Synchronization** in Principle of MLAG.

For example, when showing MAC address table on each MLAG peer devices after the system automatically completed MAC synchronization, the MAC address should be synced to each other on the MLAG peer devices.

```
admin@SwitchA# run show mac-address table
Total entries in switching table:   3
Static entries in switching table:  0
Dynamic entries in switching table: 3

VLAN      MAC address      Type         Age     Interfaces         User
----         -----------------     ---------        ----     ----------------       ------
1         08:9e:01:61:64:13   Dynamic      300      ge-1/1/2           xorp
1         cc:37:ab:4f:ad:01    Peer-Sync     300      ae1              xorp
4088      8c:ea:1b:88:5b:81    Peer-Sync     300       ae3              xorp


admin@SwitchB# run show mac-address table
Total entries in switching table:   3
Static entries in switching table:  0
Dynamic entries in switching table: 3

VLAN      MAC address      Type         Age     Interfaces         User
----         -----------------     ---------        ----     ----------------       ------
1         8c:ea:1b:88:5b:81   Dynamic      300     ae4              xorp
1         cc:37:ab:4f:ad:01    Dynamic      300      ae1              xorp
4088      08:9e:01:61:64:13    Peer-Sync      300     ae3              xorp
```

How to enable MLAG traceoptions

Use the following commands to enable MLAG traceoptions for checking the MLAG syslogs.

```
admin@Xorplus# set protocols mlag traceoptions
Possible completions:
  <[Enter]>                       Execute this command
  all                             Configure MLAG all events and packets tracing
  configuration                   Configure MLAG configuration tracing
  event                           Configure MLAG event tracing
  packet                          Configure MLAG send/receive packets tracing
  raw-packet                      Configure MLAG raw packet tracing
  state-change                    Configure MLAG state change tracing
  timer                           Configure MLAG timer tracing
```

How to ensure the reliability of the peer link?

If peer-link is down for any reason, MLAG control plane messages cannot be exchanged properly, causing the MLAG system to operate abnormally. To ensure the reliability of peer-link, note the following points when configuring and deploying peer link.

1. Only one peer link connecting the two peer devices is allowed in an MLAG domain.
2. When configuring the peer link, only one LAG port can be used as peer link.
3. Use a LAG port with at least two **directly connected** physical ports to guarantees reliable communication between the peer devices on the peer link. Use of any intermediate transmission device between the two peer devices on the peer link is not allowed. All of the directly connected physical ports should be added into one LAG port to form the peer-link. We don't support more than one L2 connection between MLAG peer switches.
4. 10G or 40G speed ports should be used for peer link to enough bandwidth is provided when the network is deployed.
5. Any manual action to shut down the peer link is strictly forbidden.

For more details, you can refer to the peer link concept in Principle of MLAG.

How to verify configurations on MLAG peer are consistent?

PICOS automatically checks the configuration consistency of the MLAG peer devices to ensure that the MLAG peer devices appear as one device to the downstream device and to make the MLAG function operate normally and smoothly.

After an MLAG related configuration is set, use the following command to show the result of MLAG configuration consistency check result.

run show mlag consistency-parameter { **link** <link-id>| **summary**}

For example,

- Show the result of per MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter link 3
Port Configurations:
-------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
MTU                      1514             1514             PASS
Mac Learning             Yes              Yes              PASS
Lag Mode                 LACP             LACP             PASS
Native Vlan              3                3                PASS
Port Vlan Mode           Access           Access           PASS

Spanning-Tree Configurations:
-------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Mode                     PVST             PVST             PASS
BPDU Guard               No               No               PASS
Root Guard               No               No               PASS
Manual Forwarding        No               No               PASS
Link Type                P2P              P2P              PASS
Instance Count           1                1                PASS
Instance Vlan 3
-- Port Priority         128              128              PASS
-- Path Cost             0                0                PASS
```

- Show the result of global MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS
Link 2  : PASS
Link 3  : PASS

MLAG Configurations:
-------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Domain ID                1                1                PASS
Node ID                  1                0                PASS
Peer VLAN                4088             4088             PASS
Link Count               3                3               PASS
Link IDs                 1   2   3       1   2   3       PASS

Spanning-Tree Configurations:
-------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   Yes              Yes              PASS
Mode                     PVST             PVST             PASS
Instance Count           65               65               PASS
```

```
Instance Vlan 1
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS

Instance Vlan 2
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS

Instance Vlan 3
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS

Instance Vlan 4
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS

DHCP Snooping Configurations:
----------------------------------------------------------------------
Property            Local Value  Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable               No          No               PASS

IGMP Snooping Configurations:
----------------------------------------------------------------------
Property                 Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS
```

In the displayed result, **Result** shows the consistency check results. The value could be **PASS** or **FAIL**:

- If **Result** is PASS, the configurations of the MLAG peer-link devices are consistent.
- If **Result** is FAIL, the configurations of the MLAG peer-link devices are inconsistent.

To ensure that the configuration parameters are consistent, we recommend that you run the MLAG consistency check command to display the configurations and the consistency check results for each MLAG peer device once you set a new MLAG related configuration.

For more details about MLAG consistency check, please refer to **MLAG Consistency Check**.

NOTE:

- Inconsistent configuration may cause MLAG to run abnormally.
- After the configuration is changed from inconsistent to consistent, you need to restart the MLAG peer devices to ensure that MLAG functions normally.

How to verify MLAG link status?

After the MLAG neighbor relationship is correctly established and MLAG link configurations are loaded on the MLAG devices, use the following command to show the MLAG link to verify the MLAG link status.

run show mlag link {*<link-id>*| **summary**}

For example,

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   ---------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

See the command reference of run show mlag link for more details about the explanation of all the output.

In the display result, if **Link Status** is not FULL or **Local Status** is not UP, you can check whether LACP neighbor is established normally between the access devices and MLAG peer device by using the command **run show lacp neighbor**.

For example,

```
admin@Xorplus# run show lacp neighbor
Aggregated interface: ae1
Port Number   Partner System ID    Partner Port Num   Port Priority   Oper Key   State
-----------   -----------------------   ----------------   -------------   --------   -----

Aggregated interface: ae2
Port Number   Partner System ID   Partner Port Num   Port Priority   Oper Key   State
-----------   -----------------------   ----------------   -------------   --------   -----
te-1/1/5      32768,3C:2C:99:89:89:01   2          32768           0x20       0x3D
```

In the displayed result, the **State** value should be **0x3D**. If not, that indicates the LACP neighbor relationship is not successfully established. Then you can check whether a packet is sent to the CoPP or check the LACP configurations.

For example,

```
admin@Xorplus# run show copp statistics forwarding-class lacp-class
lacp-class Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Input Octets..............................0

Drop rate 0 bits/sec, 0 packets/sec
Drop Packets..............................0
Drop Octets...............................0
```

How to verify MLAG neighbor status?

After completed the MLAG domain configurations, we have to check the MLAG neighbor status to make sure that the MLAG neighbor relationship is correctly established. Use the command run show mlag domain {<*domain-id*>| summary} to show the MLAG domain information, which includes the MLAG neighbor status.

For example,

```
admin@Xorplus# run show mlag domain summary
Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 0
-------------------------------------------------------------------------------------------
Peer Link  Peer IP  Peer Vlan  Neighbor Status  Config Matched  MAC Synced  # of Links
---------  --------------  ---------  ---------------    --------------      ----------  ----------
ae23       1.1.1.2    4088    ESTABLISHED      Yes       Yes         2
```

See the command reference of run show mlag domain for more details about the explanation of all the output.

If the MLAG neighbor relationship cannot be correctly established on the MLAG peer devices, the Neighbor Status is not ESTABLISHED in the display result. The possible causes and the troubleshooting procedure are as follows:

1. The peer-link connection status is abnormal. See the following link to confirm the peer-link connection status: How to verify that the peer link connection status is normal?
2. The MLAG domain configurations are incorrect or inconsistent on the MLAG peer devices, the configurations involved including domain ID, node ID and peer IP. We have to make sure the configurations are correct and consistent.

How to verify that the peer link connection status is normal?

After completed the peer link configurations, ping peer IP to verify whether the L3 connection is ok on peer link, determining the network status based on the number of Ping packets returned.

For example,

```
admin@Xorplus> ping 10.10.51.1
PING 10.10.51.1 (10.10.51.1) 56(84) bytes of data.
64 bytes from 10.10.51.1: icmp_seq=1 ttl=64 time=1.94 ms
64 bytes from 10.10.51.1: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 10.10.51.1: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 10.10.51.1: icmp_seq=4 ttl=64 time=146 ms
64 bytes from 10.10.51.1: icmp_seq=5 ttl=64 time=2.01 ms


--- 10.10.51.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.943/30.832/146.173/57.670 ms
```

How to view and clear MLAG statistics?

After MLAG is successfully deployed, you can run the MLAG statistics command to check packet statistics about MLAG. The command output helps you to determine whether data is normal or not and to locate faults.

View MLAG packet statistics of COPP:

```
admin@Xorplus# run show copp statistics forwarding-class mlag-class
mlag-class Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.....................1
Input Octets.....................153
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.....................0
Drop Octets.....................0
```

```
admin@Xorplus# run show copp statistics forwarding-class mlag-mac-sync-class
mlag-mac-sync-class Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.....................9
Input Octets.....................1511
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.....................0
Drop Octets.....................0
```

View the MLAG control plane packets statistics:

```
admin@Xorplus# run show mlag statistics
Receive:                                Transmit:
  Total Packets: 0                        Total Packets: 0
  MLAG Control: 0                         MLAG Control: 0
  MAC Sync: 0                             MAC Sync: 0
  STP Sync: 0                             STP Sync: 0
  VXLAN Sync: 0                           VXLAN Sync: 0
  Multicast Control Sync: 0               Multicast Control Sync: 0
  Configuration Consistency: 0            Configuration Consistency: 0
# of input DHCP Sync: 0                       # of Output DHCP Sync: 0
```

To collect statistics about MLAG traffic generated over a certain period, first reset the original statistics.

Clear MLAG control plane packet statistics:

```
admin@Xorplus# run clear mlag statistics
```

VLAN Configuration

- Configuring MAC-based VLAN
- MAC Trace
- Configuring Port-based VLAN

Configuring MAC-based VLAN

- Overview
- Configuring MAC-based VLAN
- Example for Configuring MAC-based VLAN
  - Networking Requirements
  - Procedure

Overview

The traditional VLAN assignment method is based on the switch access port of the traffic, MAC-based VLAN assigns VLAN based on the source MAC address of untagged traffic rather than port.

When users have the demand for security and mobility, they can configure MAC-based VLAN. MAC-based VLAN means that MAC addresses are associated with VLANs, VLAN members are defined according to the source MAC address of the packet, then the VLAN Tag is added to the packet before sending it. There is no need to re-assign VLANs when physical location changed, which improves the security and access flexibility of end users.

You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

MAC-based VLAN only handles untagged packets. Tagged packets are processed the same way as port-based VLAN.

When an untagged packet is received by the interface, the interface will look up the MAC to VLAN table entry based on the source MAC address of the packet.

- If an entry is found, the corresponding VLAN ID is assigned to the packet, and the priority value in the VLAN tag is set to 0 (zero).
- If no entries are found, the untagged packet will be forwarded in the native VLAN of the

For tagged packets, if the VLAN ID carried by the packet is in the list of VLANs allowed to be transmitted through the port, the packet is allowed to pass, otherwise the packet is dropped.

NOTEs:

- The same MAC address can be bound to no more than one VLAN.
- The number of MAC-VLAN entry supported by the whole switch varies in different switch platforms, for details please see the following attached file.

  Maximum Number of MAC VLAN Mapping on Different Platforms.xlsx
- To enable MAC-based VLAN function, add the port to the VLAN with MAC address bound. Do not forget to configure the port mode to **trunk** if there are more than one VLANs transported across this port.
- MAC-based VLAN will not work if 802.1X, voice VLAN or VXLAN is enabled on the same port.
- QinQ will not work if MAC-based VLAN is enabled.
- MAC-based VLAN can work with private VLAN.

Configuring MAC-based VLAN

Step 1 Create VLAN and add port to the VLAN.

set vlans vlan-id <*vlan-id*>

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching vlan members** <*vlan-id*>

Step 2 (Optional) Configure the port mode to **trunk**.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode** <*port-mode*>

Step 3 Configure MAC address and VLAN mapping entry.

set mac-map mac-address <*mac-address*> **vlan** <*vlan-id*>

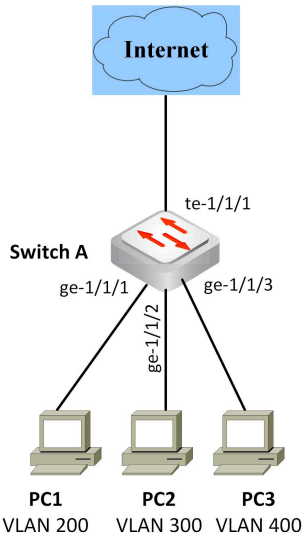
Step 4 View the configuration information of MAC-based VLAN.

run show mac-map [**mac-address** <*mac-address*>]

Example for Configuring MAC-based VLAN

Networking Requirements

Figure 1. MAC-based VLAN Configuration Example



In a company network, the network administrator divides the employees of different departments into different VLANs. In order to improve the information security in the department, only the PCs belonging to the department are allowed to access the network of the department.

As shown in Figure 1, PC1 (00:22:22:22:22:22:20), PC2 (00:33:33:33:33:20) and PC3 (00:44:44:44:44:44:20) are PCs of employees in different departments. It is required that these PCs can only access their respective department networks. If they are replaced by other PCs, they cannot access the network.

You can configure MAC-based VLAN to bind the MAC addresses of PCs in different departments to different VLANs to achieve this requirement.

Procedure

Step 1 Configure VLAN, configure port-mode to trunk port and add to VLAN.

```
admin@SwitchA# set vlans vlan-id 200
admin@SwitchA# set vlans vlan-id 300
admin@SwitchA# set vlans vlan-id 400
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@SwitchA# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 400
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 200,300,400
```

Step 2 Configure MAC address and VLAN mapping entry.

```
admin@SwitchA# set mac-map mac-address 00:22:22:22:22:20 vlan 200
admin@SwitchA# set mac-map mac-address 00:33:33:33:33:20 vlan 300
admin@SwitchA# set mac-map mac-address 00:44:44:44:44:20 vlan 400
```

Step 3 Commit the configurations.

```
admin@SwitchA# commit
```

Step 4 View the configuration information of MAC-based VLAN.

```
admin@SwitchA# run show mac-map
Total entries: 4096
MAC                 VLAN
00:22:22:22:22:20   200
00:33:33:33:33:20   300
00:44:44:44:44:20   400
```

MAC Trace

- Overview
- Configuring MAC Trace
- Configuration Example
  - Networking Requirements
  - Procedure
    - Switch A
    - Switch B
    - Switch C
  - Verification

Overview

MAC Trace function shows L2 path trace based on MAC address, which is similar to the IP layer Traceroute. It is used to detect the Ethernet link connection fault, providing an effective method for Ethernet fault detection and location.

The device determines the path by using the MAC address tables of the switches in the path.

The packets are based on CFM (IEEE802.1ag), CFM is a connection checking mechanism that uses its own Ethernet frames (its Ethernet type is 0x8902 and has its own MAC address) to verify the operational status of the service instance.

The TTL (time to live) value is 64, which specifies the lifetime of the packet and sets the maximum number of hops that the packet will go through.

NOTEs:

- To make MAC trace function work, you need to enable MAC trace function on both ends of the link under test and the intermediate devices; only after this, the devices can reply to the received MAC trace messages.
- MAC trace function supports only unicast destination MAC addresses.

Configuring MAC Trace

Step 1 Enable MAC trace function.

Enable MAC trace function on both ends of the link under test and on intermediate devices.

set tracemac disable <**true | false**>

By default, the MAC Trace function is disabled.

Only when the MAC Trace function is enabled, MAC Trace operation can be performed on the device; the device can reply to the received MAC Trace messages.

Step 2 Commit the configuration.

commit

Step 3 Perform MAC Trace detection.

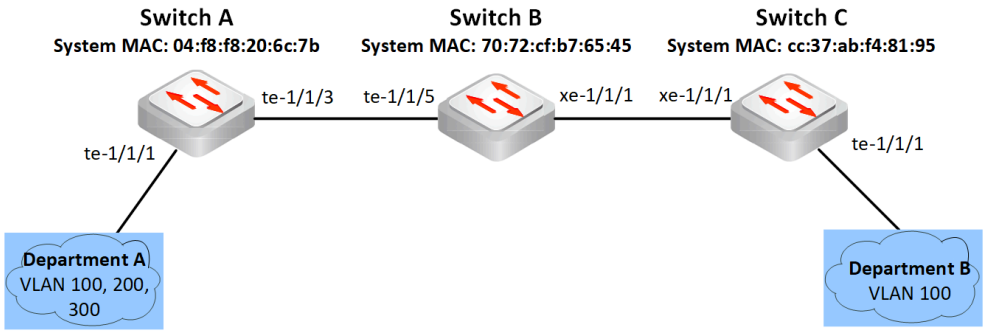
Perform MAC Trace on any end of the link under test to locate the connectivity failures between the device and the destination device.

run tracemac destination <*mac-address*> **vlan** <*vlan-id*>

Configuration Example

Networking Requirements

Figure 1. MAC Trace Configuration Example



As shown in **Figure 1**, Department A (belonging to VLAN 100, 200, 300) and Department B (belonging to VLAN 100) of a company are connected by multiple switches. This example uses command **run tracemac destination** <*mac-address*> **vlan** <*vlan-id*> to check the connectivity between the current device and the destination device, which is called a MAC Trace.

Procedure

Switch A

Step 1 Configure VLAN and port mode.

```
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 200, 300
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 100
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 200, 300
```

Step 2 Enable MAC trace function.

```
admin@SwitchA# set tracemac disable false
```

Step 3 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step 1 Configure VLAN and port mode.

```
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 100
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching vlan members 200, 300
admin@SwitchB# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchB# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching vlan members 200, 300
```

Step 2 Enable MAC trace function.

```
admin@SwitchB# set tracemac disable false
```

Step 3 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step 1 Configure VLAN and port mode.

```
admin@SwitchC# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchC# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching vlan members 200, 300
admin@SwitchC# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
```

Step 2 Enable MAC trace function.

```
admin@SwitchC# set tracemac disable false
```

Step 3 Commit the configurations.

```
admin@SwitchC# commit
```

Verification

- Run command **run show mac-address table** to check the MAC address table.
  - On Switch A:



VLAN	MAC address	Type	Age	Interfaces	User
100	22:11:11:11:11:11	Dynamic	300	te-1/1/1	xorp
100	70:72:cf:b7:65:45	Dynamic	300	te-1/1/3	xorp

  - On Switch B:

```
VLAN      MAC address          Type         Age     Interfaces          User
----      -----------------    ---------    ----    ----------------    ----------
100       04:f8:f8:20:6c:7b    Dynamic      300     te-1/1/5            xorp
100       22:11:11:11:11:11    Dynamic      300     te-1/1/5            xorp
```

- On Switch C:

```
VLAN      MAC address          Type         Age     Interfaces          User
----      -----------------    ---------    ----    ----------------    ----------
100       22:11:11:11:11:11    Dynamic      300     xe-1/1/1            xorp
100       70:72:cf:b7:65:45    Dynamic      300     xe-1/1/1            xorp
```

- On Switch C, trace MAC destination device with MAC address 20:11:11:11:11:11 and belonging to VLAN 100.

```
admin@SwitchC# run tracemac destination 22:11:11:11:11:11 vlan 100
Hop   Hostname    Ingress port     Ingress mac        Egress port    Egress mac
----  ----------- --------------   ------------       ------------   ------------
1     SwitchB       xe-1/1/1       70:72:cf:b7:65:45  te-1/1/5       70:72:cf:b7:65:45
2     SwitchA       te-1/1/3       04:f8:f8:20:6c:7b  te-1/1/1       04:f8:f8:20:6c:7b
```

Configuring Port-based VLAN

Virtual Local Area Network (VLAN) technology divides a physical LAN into multiple broadcast domains, each of which is called a VLAN. VLAN tagging (IEEE 802.1Q) is a networking standard that defines the VLAN. Hosts within a VLAN can communicate with each other but cannot communicate directly with hosts in other VLANs. Consequently, broadcast packets are confined to within a single VLAN.

You can configure a physical port as either a trunk or an access port. With the native VLAN ID, you can add the port (in trunk mode) to more than one VLAN. Access ports only belong to native VLAN, while trunk ports belong to more than one VLAN, including the native VLAN.

If hosts in different VLANs need to communicate, configure inter-VLAN communication. A VLAN interface is a Layer 3 logical interface and can implement inter-VLAN Layer 3 connectivity. Each VLAN corresponds to a VLAN interface. An IP address can be assigned to each VLAN interface. For details about VLAN interface configuration, see Layer 3 VLAN Interface Configuration.

NOTE:

When configuring VLAN member, use VLAN ID or VLAN range, but NOT other strings.

Configure the Access/Trunk Mode

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configure the Native VLAN ID

NOTE:

VLAN IDs (VLAN 1-4094) have been pre-configured in the system from version 4.3.2 and are not user-deletable. Users no longer need to use command **set vlans vlan-id** <*vlan-id*> to create VLAN IDs.

The native VLAN ID is the ID of the default VLAN (usually vlan-id 1) in which the port belongs. Every port should be included in at least one VLAN.

```
admin@XorPlus# set vlans vlan-id 5
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 5
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show vlans vlan-id 5
VLAN ID: 5
VLAN type: Static
VLAN Name: default
Description:
Vlan-interface:
Routed-interface:
Number of member ports: 1
```

```
Untagged port: ge-1/1/1
Tagged port: None
admin@XorPlus#
```

Add a Port to a VLAN with Tagged Packet

```
admin@XorPlus# set vlans vlan-id 5
admin@XorPlus# set vlans vlan-id 6
admin@XorPlus# set vlans vlan-id 7
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 5
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 6
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 7
admin@XorPlus# commit
Commit OK.
Save done.

admin@XorPlus# run show vlans
VlanID   Vlan Name     Tag        Interfaces
------    ---------  ---------  ------------------------------------------------------
1                    untagged   ge-1/1/1, ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5
                                ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                                ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                                ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                                ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, te-1/1/25
                                te-1/1/26, te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30
                     tagged
5         dafault    untagged
                     tagged     ge-1/1/2
6                    untagged
                     tagged     ge-1/1/2
7                    untagged
                     tagged     ge-1/1/2

```

Add a Port to a VLAN with Untagged Packet

```
admin@XorPlus# set vlans vlan-id 5
admin@XorPlus# set vlans vlan-id 6
admin@XorPlus# set vlans vlan-id 7
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 5 untagged
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 6 untagged
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 7 untagged
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show vlans
VlanID   Vlan Name     Tag        Interfaces
------    ---------  ---------  ------------------------------------------------------
1                    untagged   ge-1/1/1, ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5
                                ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                                ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                                ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                                ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, te-1/1/25
                                te-1/1/26, te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30
```

```
                    tagged
5         dafault   untagged    ge-1/1/2
                    tagged
6                   untagged    ge-1/1/2
                    tagged
7                   untagged   ge-1/1/2
                    tagged
```

Configuring the CPU Egress Rate Limit for an VLAN Interface

```
admin@XorPlus# set l3-interface vlan-interface vlan200 rate-limit 1024
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Creating a VLAN within the VLAN Range

```
You can create VLANs within the VLAN range, and then add ports to these VLANs.
admin@XorPlus# set vlans vlan-id 2-4094
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 1-4094
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 1-4094
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 1-4094
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

VLAN Configuration Example

In the following topology, the VLANs are configured for each switch.

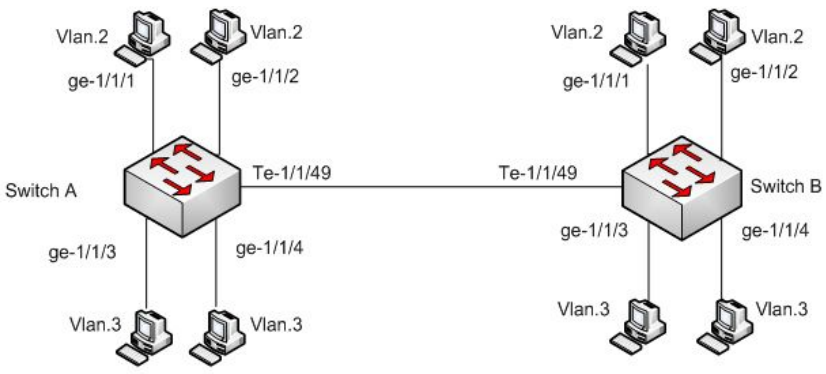


Figure 4-1.VLAN configuration.

Configuring Switch A

For Switch A, you should configure ge-1/1/1 through ge-1/1/4 as access ports and te-1/1/49 as the trunk port because the 10Gbit link will trunk the traffic of VLAN-2 and VLAN-3.

```
admin@XorPlus# set vlans vlan-id 2
```

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching port-mode trunk
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 2
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show vlans
VlanID    Vlan Name    Tag                    Interfaces
------     -----      -------- ------------------------------------------------------
1                      tagged
                       untagged     ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9,
                                    ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14,
                                    ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19,
                                    ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24,
                                    ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29,
                                    ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34,
                                    ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39,
                                    ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44,
                                    ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48, te-1/1/49,
                                    te-1/1/50, te-1/1/51, te-1/1/52,
2           default    tagged       te-1/1/49,
                       untagged     ge-1/1/1, ge-1/1/2,
3                      tagged        te-1/1/49,
                       untagged      ge-1/1/3, ge-1/1/4,
admin@XorPlus#
```

Configuring Switch B

For Switch B, configure ge-1/1/1 through ge-1/1/4 as access ports and te-1/1/49 as the trunk port because the 10 Gbit link will trunk the traffic of VLAN-2 and VLAN-3.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode access
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching port-mode trunk
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 2
admin@XorPlus#set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

```
admin@XorPlus# run show vlans
VVlanID  Vlan Name       Tag      Interfaces
------    --------     -------- ------------------------------------------------------
1                       tagged
                        untagged  ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9,
                                  ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14,
                                  ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19,
                                  ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24,
                                  ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29,
                                  ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34,
                                  ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39,
                                  ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44,
                                  ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48, te-1/1/49,
                                  te-1/1/50, te-1/1/51, te-1/1/52,
2          default      tagged    te-1/1/49,
                        untagged  ge-1/1/1, ge-1/1/2,
3                       tagged    te-1/1/49,
                        untagged   ge-1/1/3, ge-1/1/4,
```

GVRP

- Overview of GVRP
- Configuring GVRP
- Example for Configuring GVRP

Overview of GVRP

> **NOTE:**
> GVRP and MVRP are mutually exclusive which can not be configured at the same time.

To manually create or delete VLANs for all the devices in a large and complex network, the workload will be very heavy, and it is very easy to make a configuration mistakenly for network administrator. In this case, users can complete the VLAN configuration through GVRP dynamic VLAN creation function.

GARP VLAN Registration Protocol (GVRP) is an application of Generic Attribute Registration Protocol (GARP) that is used to propagate and register VLAN configuration information on interfaces among devices. After the device enables GVRP, it sends the local VLAN configuration information to other devices, and also receives VLAN configuration information from other devices, so as to dynamically updates local VLAN configuration information to keep consistent with other devices in the network, which greatly reduces the VLAN configuration work for network administrator.

When the network topology changes, GVRP re-propagates and registers VLAN configuration information according to the new topology, so as to make VLAN configuration information on all the GVRP devices be updated synchronously with the network topology.

GVRP Timer

> **NOTE:**
> It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

The supported GVRP timers are shown in the following table.

Timer Name	Function	Description
Join Timer	It is used to control the sending of Join messages.	To ensure that join messages are transmitted to other participants, an MRP participant waits for the specified period of the join timer before sending a join message. If a JoinIn message is received within one Join timer time, a second Join message is not sent; if not received, another Join message is sent.
Leave Timer	It is used to control the VLAN registrar state machine change.	The Leave timer is started when a Leave message or LeaveAll message is received on the interface. The VLAN registrar state machine waits in the Leave All state before transiting to the MT state before the Leave timer expires.
LeaveAll Timer	It is used to specify the frequency with which the Leave All state machine generates Leave All messages.	When GVRP is enabled, the device starts the LeaveAll timer. When the timer expires, the device sends a LeaveAll message externally, which is used to deregister all VLAN attributes on the GVRP device in the network.

GVRP edge-switch

For the GVRP access switch connected the host, when this switch forms a loop with other devices, it causes the GVRP messages received by this device to be forwarded cyclically over the same set of links, which consumes bandwidth and causes overutilization. To solve this problem, users can configure the following command to enable GVRP edge-switch function on the host-side switch, then the edge switch will not forward the received GVRP messages.

```
admin@PICOS# set protocols gvrp edge-switch true
admin@PICOS# commit
```

Configuring GVRP

- Configuration Notes and Constraints
- Configuring GVRP

Configuration Notes and Constraints

When configuring GVRP, pay attention to the following notes:

- GVRP and MVRP are mutually exclusive which can not be configured at the same time.
- The GVRP function can only work on **Trunk** type interfaces.
- GVRP is not allowed to be enabled on the host-side interfaces of the access devices at both ends of the network. However, users have to enable GVRP on all uplink interfaces of the access devices and all interfaces of intermediate devices.
- GVRP function conflicts with VLAN member function. That is, the static configuration of VLAN member is not allowed on the interface that enables GVRP function.
- On a single device, GVRP supports allocating up to 256 VLANs.
- STP/RSTP/MSTP blocking interface does not block GVRP PDUs.
- GVRP and Rapid PVST+ cannot be configured at the same time.
- It is not supported to deploy GVRP in MLAG topology.
- In the topology with loops, even if spanning tree is enabled, dynamic VLANs may not be removed by GVRP Leave/LeaveAll process.
- GVRP cannot be enabled on the routed interface or a member port of a LAG port.
- It is highly recommended to KEEP the default configurations of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Configuring GVRP

Step1 Enable GVRP function globally.

set protocols gvrp enable <**true | false**>

Step2 Configure the port mode to **trunk**.

set interface gigabit-ethernet *<interface-name>* **family ethernet-switching port-mode** *<port-mode>*

Step3 Enable GVRP function on a specific interface.

> **NOTE:**
> To enable GVRP function, users need to enable GVRP function BOTH globally and at the per-interface level.

set protocols gvrp interface <*interface-name*> **enable** <**true | false**>

Step4 (Optional) Enable GVRP edge-switch function on the edge switch to prevent loops.

> **NOTE:**
> This command can be enabled only on the edge switches.

set protocols gvrp edge-switch <**true | false**>

Step5 (Optional) Configure GVRP timers.

set protocols gvrp join-timer *<join-timer>*

set protocols gvrp leave-timer *<leave-timer>*

set protocols gvrp leaveall-timer*<leaveall-timer>*

Step6 Commit the configuration.

commit

Step7 View the configuration information of GVRP.

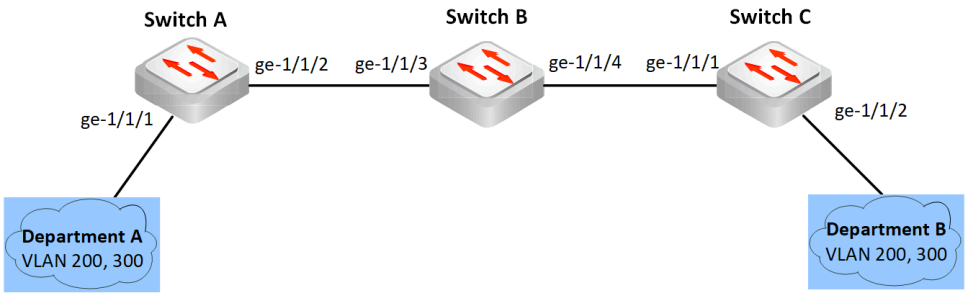
run show gvrp interface *<interface-name>*

Example for Configuring GVRP

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
- Verification

Networking Requirements

Figure 1. GVRP Configuration Example



As shown in **Figure 1**, Department A and Department B (belonging to VLAN 200, 300) of a company are connected by multiple switches, which requires mutual communication between the two departments.

We can enable GVRP function for dynamic VLAN creation to reduce the workload of VLAN configuration. To achieve GVRP dynamic VLAN registration, first statically configure the access interface of Switch A and Switch C to join VLAN 200 and 300, then enable global GVRP function and the interface GVRP function on Switch A, Switch B and Switch C.

> **NOTEs:**
> - GVRP is not allowed to be enabled on the host-side interfaces of the access devices, say ge-1/1/1 on Switch A and ge-1/1/2 on Switch C. However, GVRP needs to be enabled on ge-1/1/2 of Switch A, ge-1/1/1 of Switch C and all interfaces of Switch B .
> - The port mode of GVRP interfaces should be **Trunk** type.

Procedure

Switch A

Step1 Configure VLAN and port mode.

```
admin@SwitchA# set vlans vlan-id 200
admin@SwitchA# set vlans vlan-id 300
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
```

Step2 Enable GVRP function globally.

```
admin@SwitchA# set protocols gvrp enable true
```

Step3 Enable GVRP function on the interface.

```
admin@SwitchA# set protocols gvrp interface ge-1/1/2 enable true
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure port-mode to **trunk**.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
```

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode trunk
```

Step2 Enable GVRP function globally.

```
admin@SwitchB# set protocols gvrp enable true
```

Step3 Enable GVRP function on the interfaces.

```
admin@SwitchB# set protocols gvrp interface ge-1/1/3 enable true
admin@SwitchB# set protocols gvrp interface ge-1/1/4 enable true
```

Step4 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN and port mode.

```
admin@SwitchC# set vlans vlan-id 200
admin@SwitchC# set vlans vlan-id 300
admin@SwitchC# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
```

Step2 Enable GVRP function globally.

```
admin@SwitchC# set protocols gvrp enable true
```

Step3 Enable GVRP function on the interfaces.

```
admin@SwitchC# set protocols gvrp interface ge-1/1/1 enable true
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Verification

- After the configuration, users belonging to VLAN 200 (or 300) of department A and department B can communicate with each other.
- On Switch A, use command **run show gvrp interface** <*interface-name*> to view GVRP information on a specific interface, including GVRP Status, Registrar State, Timers and VLANs learned by the interface through GVRP.

```
admin@SwitchA# run show gvrp interface ge-1/1/2
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
ge-1/1/2        1000             10                 200

Port            Vlans Added
ge-1/1/2        200, 300
```

- On Switch A, use command **run show gvrp interface** <*interface-name*> **statistics** to view the statistics of GVRP PDUs on the interface.

```
admin@SwitchA# run show gvrp interface ge-1/1/2 statistics
packet_received: 245
packet_sent:    248
```

GVRP information on Switch B and Switch C can be viewed in the similar way and will not be repeated here.

MVRP

- Overview of MVRP
- Configuring MVRP
- Example for Configuring MVRP

Overview of MVRP

> **NOTE:**
> GVRP and MVRP are mutually exclusive and can not be configured at the same time.

To manually create or delete VLANs for all the devices in a large and complex network, the workload will be very heavy, and it is very easy to make a configuration mistakenly for network administrator. In this case, users can complete the VLAN configuration through MVRP dynamic VLAN creation function.

Multiple VLAN Registration Protocol (MVRP) is an application of Multiple Registration Protocol (MRP) that is used to propagate and register VLAN configuration information on interfaces among devices. After the device enables MVRP, it sends the local VLAN configuration information to other devices, and also receives VLAN configuration information from other devices, so as to dynamically updates local VLAN configuration information to keep consistent with other devices in the network, which greatly reduces the VLAN configuration work for network administrator.

When the network topology changes, MVRP re-propagates and registers VLAN configuration information according to the new topology, so as to make VLAN configuration information on all the MVRP devices be updated synchronously with the network topology.

MVRP Timer

> **NOTE:**
> It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

The supported MVRP timers are shown in the following table.

Timer Name	Function	Description
Join Timer	It is used to control the sending of Join messages.	To ensure that join messages are transmitted to other participants, an MRP participant waits for the specified period of the join timer before sending a join message. If a JoinIn message is received within one Join timer time, a second Join message is not sent; if not received, another Join message is sent.
Leave Timer	It is used to control the VLAN registrar state machine change.	The Leave timer is started when a Leave message or LeaveAll message is received on the interface. The VLAN registrar state machine waits in the Leave All state before transiting to the MT state before the Leave timer expires.
LeaveAll Timer	It is used to specify the frequency with which the Leave All state machine generates Leave All messages.	When MVRP is enabled, the device starts the LeaveAll timer. When the timer expires, the device sends a LeaveAll message externally, which is used to deregister all VLAN attributes on the MVRP device in the network.

MVRP edge-switch

For the MVRP access switch connected the host, when this switch forms a loop with other devices, it causes the MVRP messages received by this device to be forwarded cyclically over the same set of links, which consumes bandwidth and causes overutilization. To solve this problem, users can configure the following command to enable MVRP edge-switch function on the host-side switch, then the edge switch will not forward the received MVRP messages.

```
admin@PICOS# set protocols mvrp edge-switch true
admin@PICOS# commit
```

Configuring MVRP

- Configuration Notes and Constraints
- Configuring MVRP

Configuration Notes and Constraints

When configuring MVRP, pay attention to the following notes:

- GVRP and MVRP are mutually exclusive and can not be configured at the same time.
- The MVRP function can only work on **Trunk** type interfaces.
- VLANs need to be statically configured on the access interfaces of the access devices at both ends of the network, in order to implement MVRP bidirectional VLAN registration process.
- MVRP is not allowed to be enabled on the host-side interfaces of the access devices at both ends of the network. However, users have to enable MVRP on all uplink interfaces of the access devices and all interfaces of intermediate devices.
- MVRP function conflicts with VLAN member function. That is, the static configuration of VLAN member is not allowed on the interface that enables MVRP function.
- On a single device, MVRP supports allocating up to 256 VLANs.
- STP/RSTP/MSTP blocking interface does not block MVRP PDUs.
- MVRP and Rapid PVST+ cannot be configured at the same time.
- It is not supported to deploy MVRP in MLAG topology.
- In the topology with loops, even if spanning tree is enabled, dynamic VLANs may not be removed by MVRP Leave/LeaveAll process.
- MVRP cannot be enabled on the routed interface or a member port of a LAG port.
- It is highly recommended to KEEP the default configurations of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Configuring MVRP

Step1 Enable MVRP function globally.

set protocols mvrp enable <**true | false**>

Step2 Configure the port mode to **trunk**.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode** <*port-mode*>

Step3 Enable MVRP function on a specific interface.

> **NOTE:**
> To enable MVRP function, users need to enable MVRP function BOTH globally and at the per-interface level.

set protocols mvrp interface <*interface-name*> **enable** <**true | false**>

Step4 (Optional) Enable MVRP edge-switch function on the edge switch to prevent loops.

> **NOTE:**
> This command can be enabled only on the edge switches.

set protocols mvrp edge-switch <**true | false**>

Step5 (Optional) Configure MVRP timers.

set protocols mvrp join-timer <*join-timer*>

set protocols mvrp leave-timer <*leave-timer*>

set protocols mvrp leaveall-timer<*leaveall-timer*>

Step6 Commit the configuration.

commit

Step7 View the configuration information of MVRP.

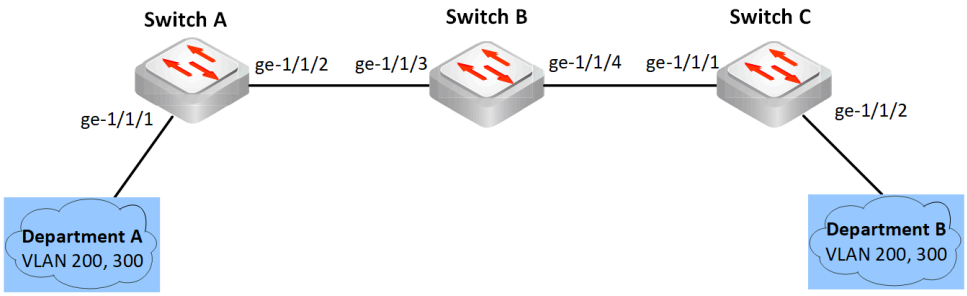
run show mvrp interface <*interface-name*>

Example for Configuring MVRP

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
- Verification

Networking Requirements

Figure 1. MVRP Configuration Example



As shown in **Figure 1**, Department A and Department B (belonging to VLAN 200, 300) of a company are connected by multiple switches, which requires mutual communication between the two departments.

We can enable MVRP function for dynamic VLAN creation to reduce the workload of VLAN configuration. To achieve MVRP dynamic VLAN registration, first statically configure the access interface of Switch A and Switch C to join VLAN 200 and 300, then enable global MVRP function and the interface MVRP function on Switch A, Switch B and Switch C.

NOTEs:

- MVRP is not allowed to be enabled on the host-side interfaces of the access devices, say ge-1/1/1 on Switch A and ge-1/1/2 on Switch C. However, MVRP needs to be enabled on ge-1/1/2 of Switch A, ge-1/1/1 of Switch C and all interfaces of Switch B .
- The port mode of MVRP interfaces should be **Trunk** type.
- VLANs need to be statically configured on the access interfaces of the access devices at both ends of the network, in order to implement MVRP bidirectional VLAN registration process.

Procedure

Switch A

Step1 Configure VLAN and port mode.

```
admin@SwitchA# set vlans vlan-id 200
admin@SwitchA# set vlans vlan-id 300
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
```

Step2 Enable MVRP function globally.

```
admin@SwitchA# set protocols mvrp enable true
```

Step3 Enable MVRP function on the interface.

```
admin@SwitchA# set protocols mvrp interface ge-1/1/2 enable true
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure port-mode to **trunk**.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode trunk
```

Step2 Enable MVRP function globally.

```
admin@SwitchB# set protocols mvrp enable true
```

Step3 Enable MVRP function on the interfaces.

```
admin@SwitchB# set protocols mvrp interface ge-1/1/3 enable true
admin@SwitchB# set protocols mvrp interface ge-1/1/4 enable true
```

Step4 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN and port mode.

```
admin@SwitchC# set vlans vlan-id 200
admin@SwitchC# set vlans vlan-id 300
admin@SwitchC# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
```

Step2 Enable MVRP function globally.

```
admin@SwitchC# set protocols mvrp enable true
```

Step3 Enable MVRP function on the interfaces.

```
admin@SwitchC# set protocols mvrp interface ge-1/1/1 enable true
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Verification

- After the configuration, users belonging to VLAN 200 (or 300) of department A and department B can communicate with each other.
- On Switch A, use command **run show mvrp interface** <*interface-name*> to view MVRP information on a specific interface, including MVRP Status, Registrar State, Timers and VLANs learned by the interface through MVRP.

```
admin@SwitchA# run show mvrp interface ge-1/1/2
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
ge-1/1/2        1000             10                  200

Port            Vlans Added
ge-1/1/2        200, 300
```

- On Switch A, use command **run show mvrp interface** <*interface-name*> **statistics** to view the statistics of MVRP PDUs on the interface.

```
admin@SwitchA# run show mvrp interface ge-1/1/2 statistics
packet_received: 245
packet_sent:    248
```

MVRP information on Switch B and Switch C can be viewed in the similar way and will not be repeated here.

Q-in-Q Basic Port Configuration

Q-in-Q tunneling allows service providers on Ethernet access networks to extend a Layer2 Ethernet connection between two customer sites. Q-in-Q tunneling can also be used to segregate or bundle customer traffic into fewer VLANs, or different VLANs, by adding another layer of 802.1Q tags.
Q-in-Q tunneling is useful when there are overlapping VLAN IDs because the 802.1Q VLAN tags are prepended by the service VLAN tag. The L2/L3 implementation of Q-in-Q tunneling supports the IEEE 802.1ad standard.
The Q-in-Q tunneling external mode belongs to basic Q-in-Q, while the Q-in-Q tunneling internal mode belongs to selective Q-in-Q.

Configuring the Q-in-Q Tunneling Internal/External Mode

By default, Q-in-Q is disabled. User can enable it as shown below:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling mode
external
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Q-in-Q Tunneling to Map Ingress VLANs to Service VLANs

Selective Q-in-Q tunneling allows user to add different customer VLAN tags based on different service VLAN tags.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# set vlans dot1q-tunneling ingress t1 from untag enabled true
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then customer-vlan 10
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then service-vlan 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
ingress t1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set vlans dot1q-tunneling ingress t2 from one-tag customer-vlan-list 20
admin@XorPlus# set vlans dot1q-tunneling ingress t2 then service-vlan 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling ingress t3 from one-tag customer-vlan-list 30
admin@XorPlus# set vlans dot1q-tunneling ingress t3 then service-vlan 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling ingress t3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1 dot1q-tunneling
Dot1q Tunneling Mode: none, Ether Type: 0x8100
Ingress: t1
Untagged-type Enabled: true
One-tagged-type Customer Vlan:
Double-tagged-type Service Vlan: 0
New Service Vlan: 100
New Customer Vlan: 10
Ingress: t2
```

```
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 20
Double-tagged-type Service Vlan: 0
New Service Vlan: 200
New Customer Vlan: 0
Ingress: t3
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 30
Double-tagged-type Service Vlan: 0
New Service Vlan: 300
New Customer Vlan: 0
admin@XorPlus#
```

Configuring Q-in-Q Tunneling Egress Pop Service VLANs

Selective Q-in-Q tunneling allows user to delete different customer VLAN tags based on different service VLAN tags.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t1 from customer-vlan 10
admin@XorPlus# set vlans dot1q-tunneling egress t1 from service-vlan 100
admin@XorPlus# set vlans dot1q-tunneling egress t1 then action none
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t1
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t2 from customer-vlan 20
admin@XorPlus# set vlans dot1q-tunneling egress t2 from service-vlan 200
admin@XorPlus# set vlans dot1q-tunneling egress t2 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t2
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t3 from customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling egress t3 from service-vlan 300
admin@XorPlus# set vlans dot1q-tunneling egress t3 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
Egress: t1
Service Vlan: 100
Customer Vlan: 10
Action: Strip both tags
Egress: t2
Service Vlan: 200
Customer Vlan: 20
Action: Retain the customer vlan tag
Egress: t3
Service Vlan: 300
Customer Vlan: 30
Action: Retain the customer vlan tag
admin@XorPlus#
```

Q-in-Q Configuration Example

The configuration of Q-in-Q is shown in Fig. 4-2.

Figure 4-2.Q-in-Q configuration.

Configuration on Provider A

Configure VLAN 100 as the default VLAN of Gigabit Ethernet ge-1/1/1, and enable the Q-in-Q tunneling internal mode on Gigabit Ethernet ge-1/1/1.
Then, configure the untagged frames received by the port with the customer VLAN tag 30 and service VLAN tag 100.
Finally, configure the customer VLAN tag 10 frames received by the port with the service VLAN tag 100.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@XorPlus# set vlans dot1q-tunneling ingress t1 from untag enabled true
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then service-vlan 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
ingress t1
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling ingress t2 from one-tag customer-vlan-list 10
admin@XorPlus# set vlans dot1q-tunneling ingress t2 then service-vlan 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t3 from customer-vlan 10
admin@XorPlus# set vlans dot1q-tunneling egress t3 from service-vlan 100
admin@XorPlus# set vlans dot1q-tunneling egress t3 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t3
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t4 from customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling egress t4 from service-vlan 100
admin@XorPlus# set vlans dot1q-tunneling egress t4 then action none
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
Ingress: t1
Untagged-type Enabled: true
One-tagged-type Customer Vlan:
Double-tagged-type Service Vlan: 0
New Service Vlan: 100
New Customer Vlan: 30
Ingress: t2
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 10
Double-tagged-type Service Vlan: 0
New Service Vlan: 100
```

```
New Customer Vlan: 0
Egress: t3
Service Vlan: 100
Customer Vlan: 10
Action: Retain the customer vlan tag
Egress: t4
Service Vlan: 100
Customer Vlan: 30
Action: Strip both tags
admin@XorPlus#
```

Configure VLAN 200 as the default VLAN of Gigabit Ethernet ge-1/1/2, and enable the Q-in-Q tunneling internal mode on Gigabit Ethernet ge-1/1/2.
Then, configure the untagged frames received by the port with the customer VLAN tag 30 and service VLAN tag 200.
Finally, configure the customer VLAN tag 20 frames received by the port with the service VLAN Tag 200.

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 200
admin@XorPlus# set vlans dot1q-tunneling ingress t5 from untag enabled true
admin@XorPlus# set vlans dot1q-tunneling ingress t5 then customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling ingress t5 then service-vlan 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
ingress t5
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling ingress t6 from one-tag customer-vlan-list 20
admin@XorPlus# set vlans dot1q-tunneling ingress t6 then service-vlan 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling ingress t6
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t7 from customer-vlan 20
admin@XorPlus# set vlans dot1q-tunneling egress t7 from service-vlan 200
admin@XorPlus# set vlans dot1q-tunneling egress t7 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
egress t7
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t8 from customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling egress t8 from service-vlan 200
admin@XorPlus# set vlans dot1q-tunneling egress t8 then action none
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
egress t8
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/2 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
Ingress: t5
Untagged-type Enabled: true
One-tagged-type Customer Vlan:
Double-tagged-type Service Vlan: 0
New Service Vlan: 200
New Customer Vlan: 30
Ingress: t6
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 20
Double-tagged-type Service Vlan: 0
New Service Vlan: 200
New Customer Vlan: 0
Egress: t7
Service Vlan: 200
Customer Vlan: 20
Action: Retain the customer vlan tag
Egress: t8
Service Vlan: 200
Customer Vlan: 30
Action: Strip both tags
admin@XorPlus#
```

Configure VLAN 100/200 as the trunk port of Gigabit Ethernet te-1/1/49, and enable the Q-in-Q tunneling internal mode.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet te-1/1/49 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
```

Configuration on Provider B

Configure VLAN 100 as the default VLAN of Gigabit Ethernet ge-1/1/1, and enable the Q-in-Q tunneling internal mode on Gigabit Ethernet ge-1/1/1.
Then, configure the untagged frames received by the port with the customer VLAN tag 30 and service VLAN tag 100.
Finally, configure the customer VLAN tag 10 frames received by the port with the service VLAN tag 100.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@XorPlus# set vlans dot1q-tunneling ingress t1 from untag enabled true
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling ingress t1 then service-vlan 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
ingress t1
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling ingress t2 from one-tag customer-vlan-list 10
admin@XorPlus# set vlans dot1q-tunneling ingress t2 then service-vlan 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t3 from customer-vlan 10
admin@XorPlus# set vlans dot1q-tunneling egress t3 from service-vlan 100
admin@XorPlus# set vlans dot1q-tunneling egress t3 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t3
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t4 from customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling egress t4 from service-vlan 100
admin@XorPlus# set vlans dot1q-tunneling egress t4 then action none
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling
egress t4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
Ingress: t1
Untagged-type Enabled: true
One-tagged-type Customer Vlan:
Double-tagged-type Service Vlan: 0
New Service Vlan: 100
New Customer Vlan: 30
Ingress: t2
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 10
Double-tagged-type Service Vlan: 0
New Service Vlan: 100
New Customer Vlan: 0
Egress: t3
Service Vlan: 100
Customer Vlan: 10
Action: Retain the customer vlan tag
Egress: t4
Service Vlan: 100
```

```
Customer Vlan: 30
Action: Strip both tags
admin@XorPlus#
```

Configure VLAN 200 as the default VLAN of Gigabit Ethernet ge-1/1/2, and enable the Q-in-Q tunneling internal mode on Gigabit Ethernet 1/1/2.
Then, configure the untagged frames received by the port with the customer VLAN tag 30 and service VLAN tag 200.
Finally, configure the customer VLAN tag 20 frames received by the port with the service VLAN Tag 200.

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 200
admin@XorPlus# set vlans dot1q-tunneling ingress t5 from untag enabled true
admin@XorPlus# set vlans dot1q-tunneling ingress t5 then customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling ingress t5 then service-vlan 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
ingress t5
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling ingress t6 from one-tag customer-vlan-list 20
admin@XorPlus# set vlans dot1q-tunneling ingress t6 then service-vlan 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling ingress t6
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t7 from customer-vlan 20
admin@XorPlus# set vlans dot1q-tunneling egress t7 from service-vlan 200
admin@XorPlus# set vlans dot1q-tunneling egress t7 then action one
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
egress t7
admin@XorPlus# commit
admin@XorPlus# set vlans dot1q-tunneling egress t8 from customer-vlan 30
admin@XorPlus# set vlans dot1q-tunneling egress t8 from service-vlan 200
admin@XorPlus# set vlans dot1q-tunneling egress t8 then action none
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling
egress t8
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching dot1q-tunneling mode
internal
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/2 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
Ingress: t5
Untagged-type Enabled: true
One-tagged-type Customer Vlan:
Double-tagged-type Service Vlan: 0
New Service Vlan: 200
New Customer Vlan: 30
Ingress: t6
Untagged-type Enabled: false
One-tagged-type Customer Vlan: 20
Double-tagged-type Service Vlan: 0
New Service Vlan: 200
New Customer Vlan: 0
Egress: t7
Service Vlan: 200
Customer Vlan: 20
Action: Retain the customer vlan tag
Egress: t8
Service Vlan: 200
Customer Vlan: 30
Action: Strip both tags
admin@XorPlus#
```

Configure VLAN 100/200 as the trunk port of Gigabit Ethernet te-1/1/49, and enable the Q-in-Q tunneling internal mode.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
```

```
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet te-1/1/49 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
admin@XorPlus#
```

Private VLAN Configuration Guide

- Introduction of PVLAN
- Configuration Notes of PVLAN
- Configuring PVLAN
- Example for Configuring PVLAN
- Example for Configuring DHCP Snooping with PVLAN

Introduction of PVLAN

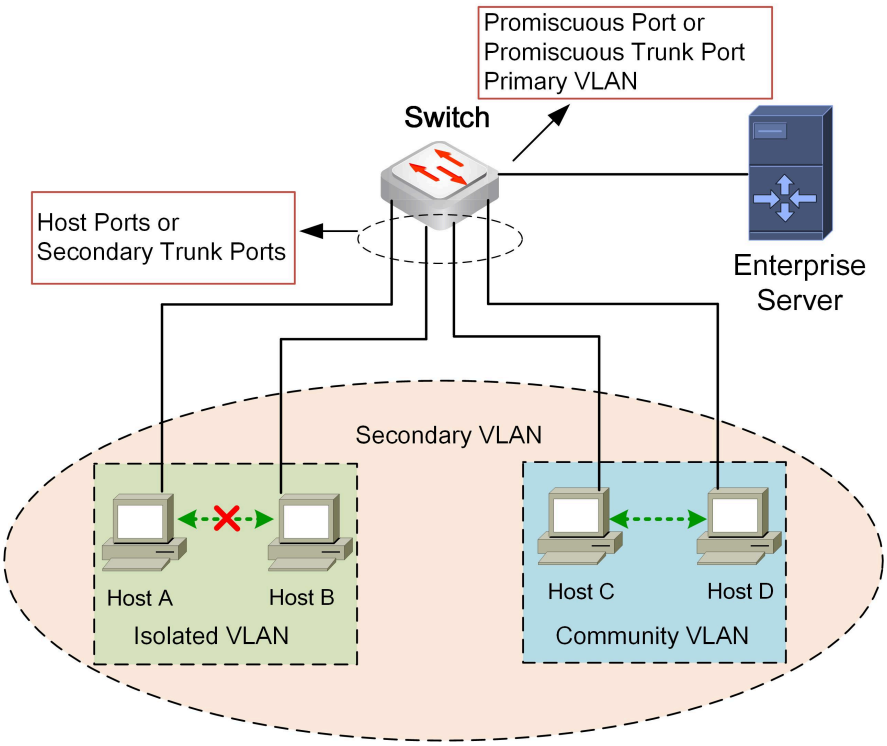
- Overview
- PVLAN Concepts and Terminology
  - PVLAN Types
  - PVLAN Port Modes
- Communication Restriction between PVLAN Ports
- Configuration Synchronization for PVLAN Port
- MAC Address Duplication
- PVLAN Across Multiple Switches
- Deploy DHCP Snooping with PVLAN
  - DHCP Client and DHCP Server Deployed on a Single Switch
  - DHCP Client and Server Deployed Across Multiple Switches

Overview

Private VLAN (PVLAN) is a technology that divides a VLAN broadcast domain into multiple discrete broadcast subdomains by defining secondary VLANs (community VLANs and an isolated VLAN) inside a primary VLAN, achieving port isolation within a VLAN while sharing a single layer-3 router port and the same IP subnet.

For example, in **Figure 1**, access-side VLANs are divided into Isolated VLAN and Community VLAN. Community VLAN users can communicate with each other, while Isolated VLAN users are isolated and cannot communicate with each other. However, both Community VLAN users and Isolated VLAN users can access the Primary VLAN where the enterprise servers are located. All of this can be accomplished by deploying PVLAN.

Figure 1. PVLAN Application Diagram



PVLAN has the following characteristics and advantages,

- By deploying PVLANs and configuring isolated VLANs on the access side, it is possible to isolate the traffic of different users in the same VLAN. This improves the network security as well as conserving VLANs.
- As all secondary VLAN users inside a primary VLAN share one IP subnet, PVLAN can be deployed to conserve IP addresses.

PVLAN Concepts and Terminology

PVLAN Types

PVLAN defines two VLAN types: primary VLAN and secondary VLAN. One pair of PVLAN consists of only one primary VLAN and at least one secondary VLAN. One switch can configure multiple pairs of PVLAN.

Note that, secondary VLANs need to be associated with a primary VLAN to form a pair of PVLANs.

- **Primary VLAN**

Ports within a primary VLAN are connected to the uplink devices, and the corresponding ports are PVLAN promiscuous ports or promiscuous trunk ports. These ports are used to transmit traffic from the promiscuous ports to the host ports and to other promiscuous ports.

A pair of PVLAN has only one primary VLAN.

A primary VLAN can be associated with multiple community VLANs and only one isolated VLAN.

- **Secondary VLAN**

Ports within a secondary VLAN are connected to the hosts or downlink devices, and the corresponding ports are PVLAN host ports or secondary trunk ports. These ports are used to transmit traffic from hosts to other allowed hosts or to upstream routers.

There are two types of secondary VLANs: Isolated VLAN and Community VLAN.

Secondary VLANs should be configured to associate with a primary VLAN. One secondary VLAN (isolated or community) can be associated with only one primary VLAN.

> **NOTE:**
>
> In the CLI configuration, the configurable values are "**isolated**" and "**community**", but not "**secondary**".

- **Isolated VLAN**

An isolated VLAN is a secondary VLAN, which is used to transmit traffic from the hosts toward the promiscuous ports and the gateway. Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level. Traffic received from an isolated port is forwarded only to promiscuous ports.

A pair of PVLAN can configure not more than one Isolated VLAN.

- **Community VLAN**

A community VLAN is a secondary VLAN that transmits upstream traffic from the host ports to the promiscuous port gateways and to other host ports in the same community VLAN. Ports within a community VLAN can communicate with each other and the primary VLAN but cannot communicate with ports in other communities at the Layer 2 level or isolated VLAN.

Users can configure multiple community VLANs in a pair of PVLAN.

PVLAN Port Modes

Ethernet interfaces are classified into four PVLAN types depending on the devices connected to them and the way they process the frames.

> **NOTE:**
>
> - Only when configured with the PVLAN port mode, a port can be added into a PVLAN.
> - After modifying the port mode, the port will be restarted automatically.

- **PVLAN Host Port**

A PVLAN host port connects to a user device. For host mode ports, make sure that their native VLAN is a secondary VLAN, otherwise the ports won't be able to forward packets from primary VLAN. One host port can be added into only one secondary VLAN.

Packets sent from this port are untagged.

- **PVLAN Secondary Trunk Port**

A PVLAN secondary trunk port is used to connect to the downstream devices. One secondary trunk port can be added into more than one secondary VLAN. Secondary trunk mode is applicable to scenarios where multiple secondary VLANs need to pass through the downlink port while Host mode is applicable to cases where only one secondary VLAN passes through the downlink port.

The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the secondary trunk mode port, thus masking the primary VLAN for the downstream device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> - Secondary trunk mode ports can be added to only one secondary VLAN of the same primary VLAN, but can be added to multiple secondary VLANs associated with different primary VLANs.
> - PVLAN secondary trunk port can also be added to normal VLANs in addition to the secondary VLANs.

- **PVLAN Promiscuous Port**

PVLAN promiscuous ports are used to connect to the uplink devices. Uplinks are typically ports that connect to routers, firewalls, servers or provider networks.

Promiscuous ports belong to the primary VLAN, which can communicate with all PVLAN ports, including host/secondary trunk ports and other promiscuous/promiscuous trunk ports within the same primary VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.

Make sure that the native VLAN of the promiscuous port is the primary VLAN, otherwise the port will not forward packets sent from a secondary VLAN.

Promiscuous port mode is used when there is only one primary VLAN passing through the uplink port. Packets sent from this port are untagged.

- **PVLAN Promiscuous Trunk Port**

PVLAN promiscuous trunk ports are used to connect to the uplink devices. Promiscuous trunk port mode is used when there are more than one primary VLAN passing through the uplink port.

The secondary VLAN ID carried by the message is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the uplink device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> PVLAN Promiscuous trunk ports can also be added to normal VLANs in addition to the primary VLANs.

Communication Restriction between PVLAN Ports

PVLANs limit the Layer 2 communication within a pair of Private VLANs, a port defined in a PVLAN cannot communicate with ports in other pairs of PVLANs or normal VLANs.

The following table summaries the Layer 2 communication restriction between the PVLAN ports.

PVLAN	PVLAN Mode	Port Mode	Communication Restriction

Primary VLAN	Primary VLAN	Promiscuous Port Promiscuous Trunk Port	The port within the primary VLAN can communicate with all ports in a pair of PVLAN.
Secondary VLAN	Isolated VLAN	Host Port Secondary Trunk Port	Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level. Each isolated VLAN must be bound to a primary VLAN.
	Community VLAN	Host Port Secondary Trunk Port	Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level. Each community VLAN must be bound to a primary VLAN.

Configuration Synchronization for PVLAN Port

In order for users in the secondary VLAN to communicate with users in the Primary VLAN, the system synchronizes Private VLAN configurations for the PVLAN ports.

If the PVLAN port has been configured to add to the primary VLAN (or secondary VLAN), the port will be added to the corresponding secondary VLAN (or primary VLAN) based on the following rules while maintaining the original configuration.

- The downlink ports in host mode or secondary trunk mode will be added to the corresponding primary VLAN. The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the port, thus masking the primary VLAN for the downstream device.

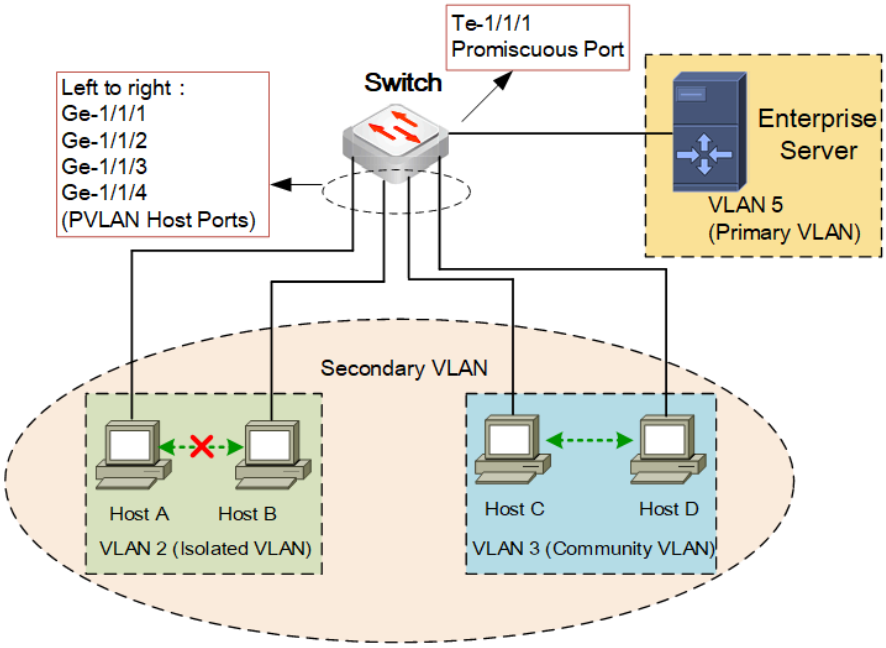
Messages sent from the secondary trunk mode ports could be tagged or untagged, which is determined by the tagged/untagged configuration of the secondary VLAN.

- The uplink ports in promiscuous mode or promiscuous trunk mode will be added to the corresponding secondary VLAN. The secondary VLAN ID carried by the packets is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the upstream device.

Messages sent from the promiscuous trunk mode ports could be tagged or untagged, which is determined by the tagged/untagged configuration of the primary VLAN.

The following example illustrates configuration synchronization for PVLAN ports in detail.

Figure 2. Diagram for Configuration Synchronization for PVLAN Ports



To configure the topology shown above:

```
set vlans vlan-id 2 private-vlan mode isolated
set vlans vlan-id 3 private-vlan mode community
set vlans vlan-id 5 private-vlan mode primary
set vlans vlan-id 5 private-vlan association 2-3
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode pvlan-promiscuous
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 5
```

The system will synchronize private VLAN configurations for the PVLAN ports after completing the configuration, as shown in the following table.

Port	Port Mode	Native VLAN	VLANs Allowed to Pass

Ge-1/1/1	pvlan-host	2	• Added to VLAN 2, 5 • Allow packets of VLAN 2, 5 to pass
Ge-1/1/2	pvlan-host	2	• Added to VLAN 2, 5 • Allow packets of VLAN 2, 5 to pass
Ge-1/1/3	pvlan-host	3	• Added to VLAN 3, 5 • Allow packets of VLAN 3, 5 to pass
Ge-1/1/4	pvlan-host	3	• Added to VLAN 3, 5 • Allow packets of VLAN 3, 5 to pass
Te-1/1/1	pvlan-promiscuous	5	• Added to VLAN 2, 3, 5 • Allow packets of VLAN 2, 3, 5 to pass

Users can run the command **run show vlans** to view the VLAN information. In the output, synchronized VLANs of the PVLAN ports are marked with a **(pv).**

```
admin@Xorplus# run show vlans
VlanID  Vlan Name    Tag        Interfaces
------  ------------ --------   ------------------------------------------------------
2       default      untagged   ge-1/1/1, ge-1/1/2, te-1/1/1(pv)
                     tagged
3       default      untagged   ge-1/1/3, ge-1/1/4, te-1/1/1(pv)
                     tagged
5       default      untagged   ge-1/1/1(pv), ge-1/1/2(pv), ge-1/1/3(pv), ge-1/1/4(pv)
                     tagged
```

MAC Address Duplication

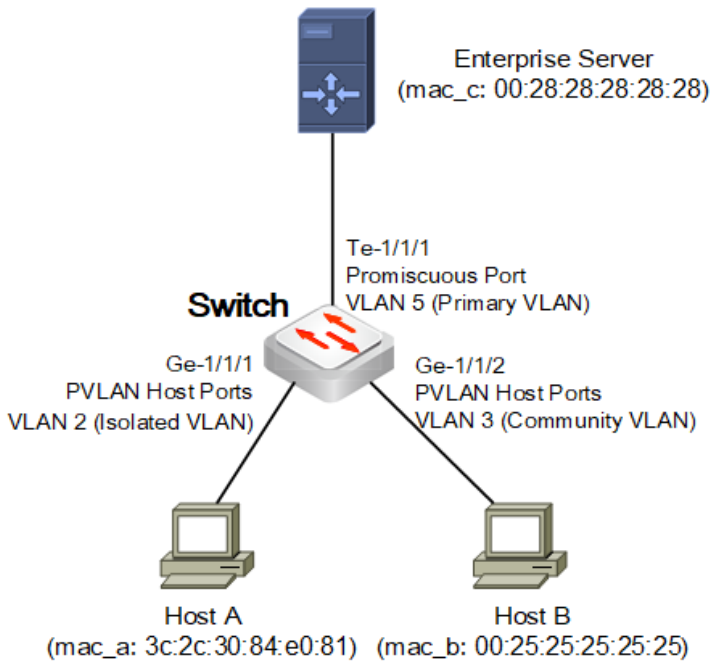
To avoid flooding of packets received from the PVLAN port, PVLAN performs MAC address duplication, including:

- Secondary VLAN to Primary VLAN duplication, that is, MAC addresses dynamically learned or statically configured on ports in the Secondary VLAN are duplicated to the corresponding Primary VLAN.
- Primary VLAN to Secondary VLAN duplication, that is, MAC addresses dynamically learned or statically configured on ports in the Primary VLAN are duplicated to all the corresponding Secondary VLANs.

Note that, for the normal trunk ports between two or multiple switches, MAC addresses dynamically learned or statically configured on ports in the private VLAN will also be duplicated following the rules stated above.

The following example illustrates PVLAN MAC address duplication in detail.

Figure 3. Diagram for PVLAN MAC Address Duplication



From the topology shown above, the resulting MAC address tables before and after the duplication are shown below.

MAC Address Table Before MAC Duplication

Source MAC Address	VLAN	Outgoing Interface

mac_c	5	Te-1/1/1
mac_a	2	Ge-1/1/1
mac_b	3	Ge-1/1/2

MAC Address Table After MAC Duplication

Source MAC Address	VLAN	Outgoing Interface
mac_c	5	Te-1/1/1
mac_c	2	Te-1/1/1
mac_c	3	Te-1/1/1
mac_a	2	Ge-1/1/1
mac_a	5	Ge-1/1/1
mac_b	3	Ge-1/1/2
mac_b	5	Ge-1/1/2

Users can run the command **run show mac-address table** to view the MAC address table. In the output, duplicated MAC address entries are marked with a **(pv)**.

```
admin@Xorplus# run show mac-address table
Total entries in switching table:   7
Static entries in switching table:  0
Dynamic entries in switching table: 7

VLAN    MAC address            Type         Age     Interfaces    User
----      -----------------    ---------    ----    -----------   ----------
5         00:28:28:28:28:28    Dynamic      300     te-1/1/1       xorp
2         00:28:28:28:28:28    Dynamic(pv)  300     te-1/1/1       xorp
3         00:28:28:28:28:28    Dynamic(pv)  300     te-1/1/1       xorp
2         3c:2c:30:84:e0:81    Dynamic      300     ge-1/1/1       xorp
5         3c:2c:30:84:e0:81    Dynamic(pv)  300     ge-1/1/1       xorp
3         00:25:25:25:25:25    Dynamic      300     ge-1/1/2       xorp
3         00:25:25:25:25:25    Dynamic(pv)  300     ge-1/1/2       xorp
```

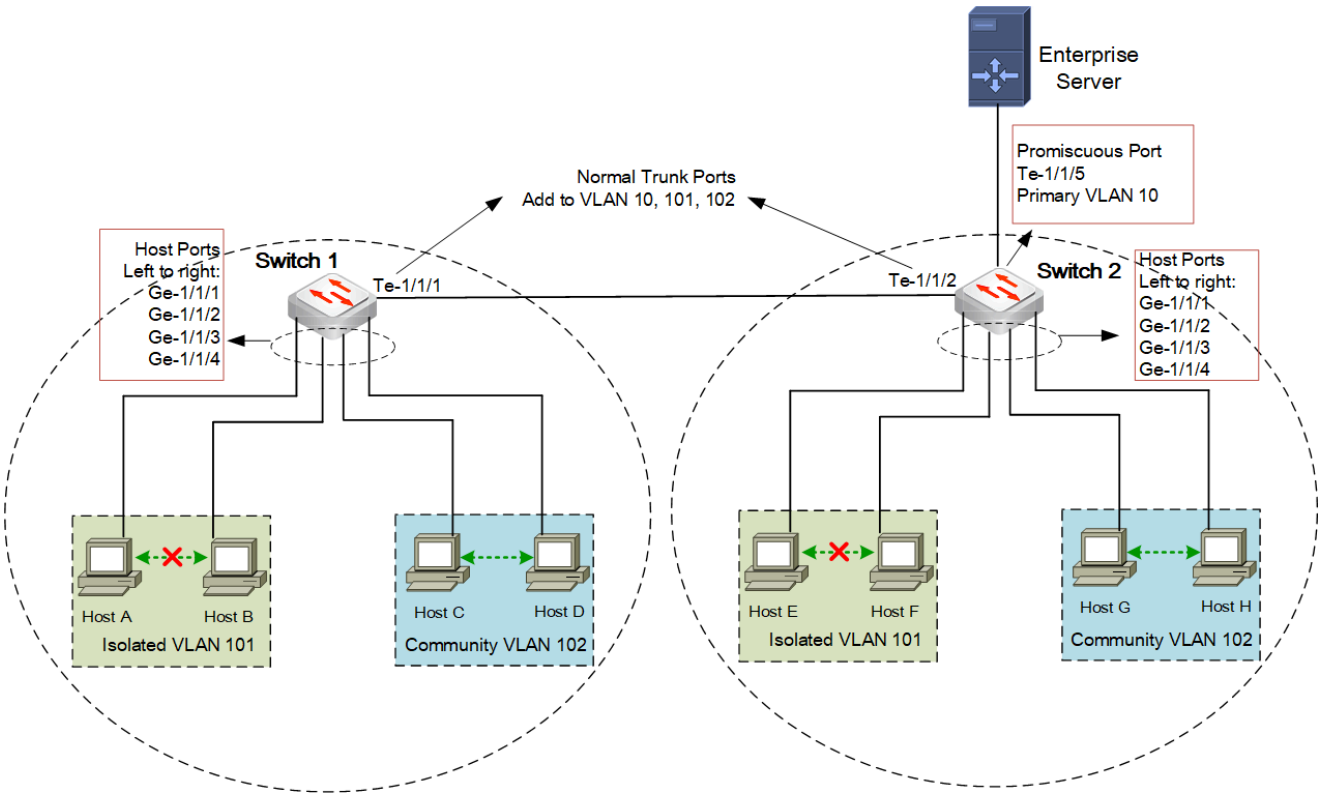
NOTE:
For the secondary VLANs configured on the normal trunk port, the static MAC entries configured on these secondary VLANs are NOT duplicated to the primary VLAN.

However, for the primary VLAN configured on the normal trunk port, the static MAC entries configured on this primary VLAN are duplicated to the secondary VLANs.

PVLAN Across Multiple Switches

Users can configure normal trunk ports between two or multiple switches to enable PVLAN cross-device communication.

Figure 4. Diagram for PVLAN Across Multiple Switches



As shown in the topology above, we want to achieve the following:

- Hosts connecting to the same switch or across multiple switches in the same Community VLAN can communicate with each other. In the figure, Host C, Host D, Host G and Host H in the same Community VLAN (VLAN 102) can communicate with each other.
- Hosts connecting to the same switch or across multiple switches in the same Isolated VLAN cannot communicate with each other. In the figure, Host A, Host B, Host E and Host F in the same Isolated VLAN (VLAN 101) cannot communicate with each other.

Besides the basic PVLAN configurations, we have to configure ports Te-1/1/1 and Te-1/1/2 as normal trunk ports, connecting Switch 1 to Switch 2. And then add Te-1/1/1 and Te-1/1/2 to all the private VLAN IDs (VLAN 10, 101 and 102 in this example) and normal VLAN IDs (if have) to carry packets needed to forward through the trunk link.

To configure the topology shown above:

```
# Switch 1
set vlans vlan-id 10 private-vlan mode primary
set vlans vlan-id 102 private-vlan mode community
set vlans vlan-id 101 private-vlan mode isolated
set vlans vlan-id 10 private-vlan association 101-102
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 101
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 101
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 102
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 102
set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 10
set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 101-102
```

```
# Switch 2
set vlans vlan-id 10 private-vlan mode primary
set vlans vlan-id 102 private-vlan mode community
set vlans vlan-id 101 private-vlan mode isolated
set vlans vlan-id 10 private-vlan association 101-102
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode pvlan-host
set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode pvlan-promiscuous
set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 101
```

```
set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 101
set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 102
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 102
set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 10
set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 10
set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 101-102
```

From the configurations above, we can note that PVLAN configurations, as well as the binding configuration of primary VLAN and secondary VLAN need to be consistent on all switches.

Deploy DHCP Snooping with PVLAN

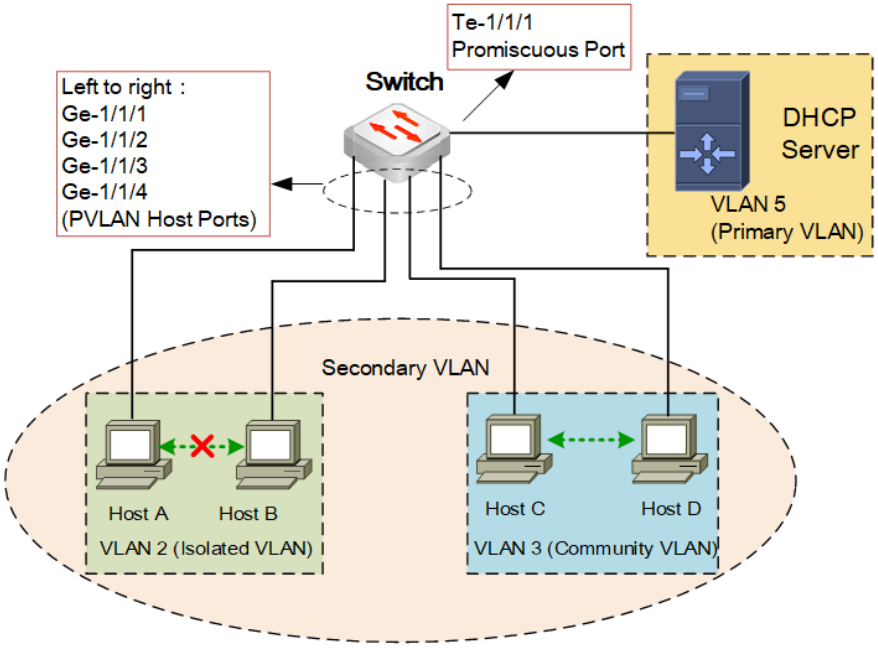
PicOS supports deploying DHCP snooping in a PVLAN topology. Depending on whether the DHCP client and server are on the same PVLAN switch, this section is divided into two parts:

- DHCP Client and Server Deployed on a Single Switch
- DHCP Client and Server Deployed Across Multiple Switches

DHCP Client and DHCP Server Deployed on a Single Switch

In the following PVLAN topology, Switch acts as a user gateway and forwards DHCP messages to the DHCP server, so that DHCP clients Host A, Host B, Host C and Host D can request for IP address lease and other related configuration information from the DHCP server. In order to provide better service to DHCP users, network administrators can configure DHCP Snooping to prevent DHCP attacks.

Figure 5. Diagram for Deploying DHCP Snooping with PVLAN on a Single Switch



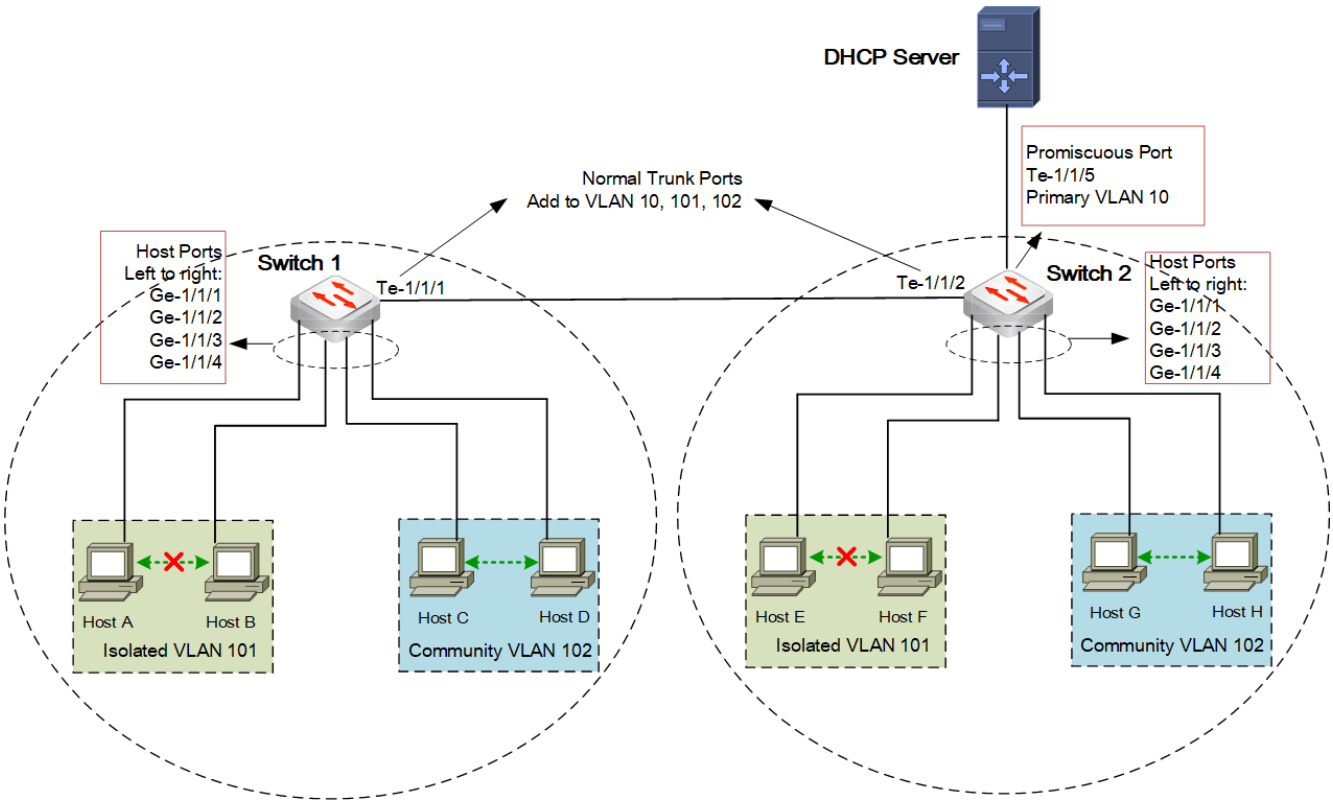
In the above topology, besides the basic PVLAN configurations, you need to do the following DHCP snooping configuration to enable DHCP snooping and configure the trust port.

```
set protocols dhcp snooping vlan 5 disable false
set protocols dhcp snooping trust-port te-1/1/1
```

DHCP Client and Server Deployed Across Multiple Switches

In the following PVLAN topology, DHCP clients Host A, Host B, Host C, Host D and the DHCP server are deployed across two PVLAN switches.

Figure 6. Diagram for Deploying DHCP Snooping with PVLAN Across Multiple Switches



In this example, you can refer to PVLAN Across Multiple Switches to complete the basic PVLAN configurations. When configuring DHCP snooping, pay attention to the following points:

- Enable DHCP snooping in VLAN 10 on both Switch 1 and Switch 2.
- In addition to configuring port Te-1/1/5 on Switch 2 as a trust port, which is connected to the DHCP server, users also have to configure Te-1/1/1 on Switch 1 as a trust port.

Configuration Notes of PVLAN

When configuring PVLAN on a device, pay attention to the following points:

- One pair of PVLAN consists of only one primary VLAN and at least one secondary VLAN. One switch can configure multiple pairs of PVLAN.
- One primary VLAN can be associated with multiple community VLANs and only one isolated VLAN.
- A secondary VLAN (isolated or community) can be associated with one and only one primary VLAN, but not multiple primary VLANs.
- PVLAN supports to be deployed in conjunction with MSTP or rapid PVST+. A pair of primary VLAN and secondary VLANs should be in the same MSTP instance when MSTP is deployed with PVLAN.
- PVLAN supports to be deployed with DHCP snooping.
- Both primary VLAN and secondary VLAN should be in the same MSTP instance when MSTP is deployed with PVLAN.
- Layer 3 routing on private VLAN is not supported.
- VLAN 1 is not allowed to be configured as a private VLAN.
- If you want to change a private VLAN to a normal VLAN, you need to remove the configurations for PVLAN-related binding relationship before you can remove the PVLAN mode configuration. For example, if you use the **set vlans vlan-id** <*vlan-id*> **private-vlan association** <*secondary-vlan-list*> command for PVLAN association, remove the binding relationship first before you can change the private VLAN to a normal VLAN.

  Similarly, it is also required to remove the private VLAN related configuration (e.g. static MAC address configurations on private VLAN) before changing the role of a private VLAN to another PVLAN type, e.g. when changing the PVLAN type from primary VLAN to secondary VLAN.
- Before modifying or deleting PVLAN association configuration, you need to delete all the PVLAN settings of the involved Private VLANs.
- For the secondary VLANs configured on the normal trunk port, the static MAC entries configured on these secondary VLANs are NOT duplicated to the primary VLAN. However, for the primary VLAN configured on the normal trunk port, the static MAC entries configured on this primary VLAN are duplicated to the secondary VLANs.

Configuring PVLAN

By default, the Private VLAN is disabled. To configure a PVLAN, follow these steps:

1. Create the secondary VLANs, i.e. isolated VLAN or community VLAN.
2. Create the primary VLAN.
3. Associate the secondary VLAN with the primary VLAN. (Only one isolated VLAN can be associated with a primary VLAN, but more than one community VLAN can be associated with a primary VLAN).
4. Configure the port connected to the host or the downlink devices as a PVLAN host port or secondary trunk port.
5. Configure the port connected to the uplink device as a PVLAN promiscuous port or promiscuous trunk port.
6. Add PVLAN ports to the private VLAN and set the native VLAN of the port as the private VLAN.
7. Verify PVLAN configurations.

Procedure

Step1 Create the secondary VLANs.

set vlans vlan-id <*vlan-id*> **private-vlan mode community**

set vlans vlan-id <*vlan-id*> **private-vlan mode isolated**

Step2 Create the primary VLAN.

set vlans vlan-id <*vlan-id*> **private-vlan mode primary**

Step3 Associate the secondary VLAN with the primary VLAN.

set vlans vlan-id <*vlan-id*> **private-vlan association** <*secondary-vlan-list*>

Step4 Configure the port connected to the uplink device as a promiscuous port or promiscuous trunk port.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode** <*port-mode*>

Step5 Configure the port connected to the host or the downlink device as a host port or secondary trunk port.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode** <*port-mode*>

Step6 Add the PVLAN ports to the private VLAN and set the native VLAN of the port as the private VLAN.

set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

Step7 Commit the configurations.

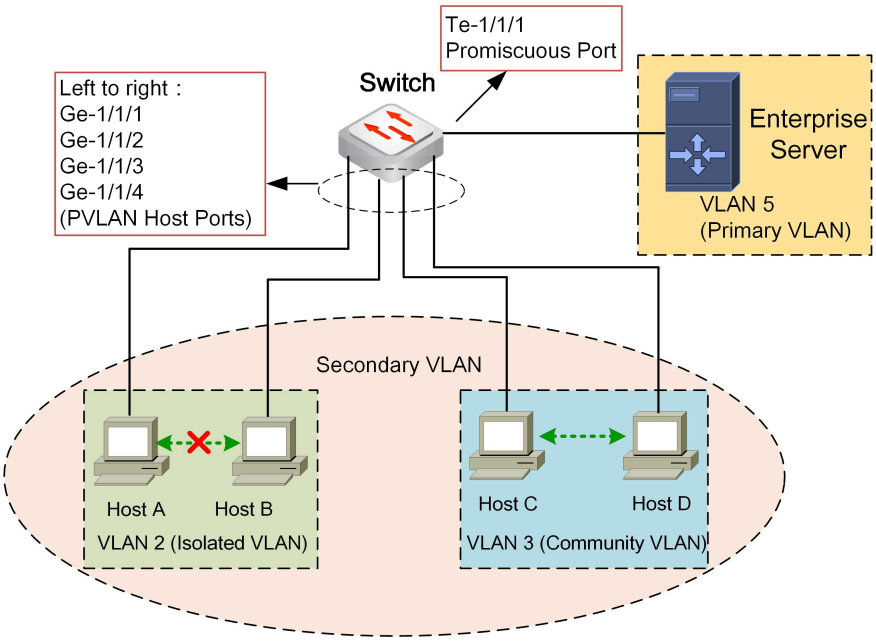
Commit

Example for Configuring PVLAN

- Networking Requirements
  - Figure 1. PVLAN Configuration Example
- Procedure
- Verify the Configuration

Networking Requirements

Figure 1. PVLAN Configuration Example



As shown in **Figure 1**, in an enterprise network, all employees have access authorization to the enterprise server. However, it is desirable that some employees within the enterprise can communicate with each other, while some employees are isolated from each other.

In order to achieve this, PVLAN feature can be deployed on the switch that connects the terminal and the enterprise server. PVLAN not only meets the network isolation demands, but also addresses the problem of VLAN ID shortage, and is easy to maintain by the network administrator.

Complete the following configurations on the Switch:

- To isolate the communication between Host A and Host B, configure the VLAN of Host A and Host B (VLAN 2) as the Isolated VLAN; To make sure Host C and Host D can communicate with each other, configure the VLAN of Host C and Host D (VLAN 3) as the Community VLAN.
- Configure the VLAN of the server as the Primary VLAN.
- The access ports of Host A, Host B, Host C, and Host D are configured as the PVLAN host ports.
- Add the access ports of Host A and Host B (ge-1/1/1 and ge-1/1/2) into Isolated VLAN. Add the access ports of Host C and Host D (ge-1/1/3 and ge-1/1/4) to the Community VLAN.
- The port connected to the server is configured as promiscuous port and is added into the primary VLAN (VLAN 5).

Procedure

Step1 Create the secondary VLANs.

```
admin@XorPlus# set vlans vlan-id 2 private-vlan mode isolated
admin@XorPlus# set vlans vlan-id 3 private-vlan mode community
```

Step2 Create the primary VLAN.

```
admin@XorPlus# set vlans vlan-id 5 private-vlan mode primary
```

Step3 Associate the secondary VLAN with the primary VLAN.

```
admin@XorPlus# set vlans vlan-id 5 private-vlan association 2-3
```

Step4 Configure the ports connected to the hosts as the PVLAN host ports.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode pvlan-host
```

Step5 Configure the port connected to the Server as the promiscuous port.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode pvlan-promiscuous
```

Step6 Add the host ports into the secondary VLAN and set the native VLAN of the host port as the secondary VLAN ID.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
```

Step7 Add the promiscuous port into the primary VLAN and set the native VLAN of the promiscuous port as the primary VLAN ID.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 5
```

Step8 Commit the configurations.

```
admin@XorPlus# commit
```

Verify the Configuration

- You can use the **run show vlans private-vlan** command to view the PVLAN configuration information.

```
admin@Xorplus# run show vlans private-vlan
Primary   Secondary  Type            Tag         Interfaces
-------   ---------  -----------     --------    -------------------------
5                    primary         untagged    te-1/1/1
                                       tagged
          2          isolated        untagged    ge-1/1/1, ge-1/1/2
                                       tagged
          3          community       untagged    ge-1/1/3, ge-1/1/4
                                       tagged
```

- You can use the **run show vlans private-vlan type** command to view the PVLAN type information.

```
admin@Xorplus# run show vlans private-vlan type
Vlan Type
---- -----------
5    primary
2    isolated
3    community
```

- Check device connection status.

The Server, Host A, Host B, Host C and Host D are on the same subnet.

Host A, Host B, Host C and Host D can communicate with the Server.

Host A and Host B cannot communicate with each other at Layer 2.

Host C and Host D can communicate with each other at Layer 2.

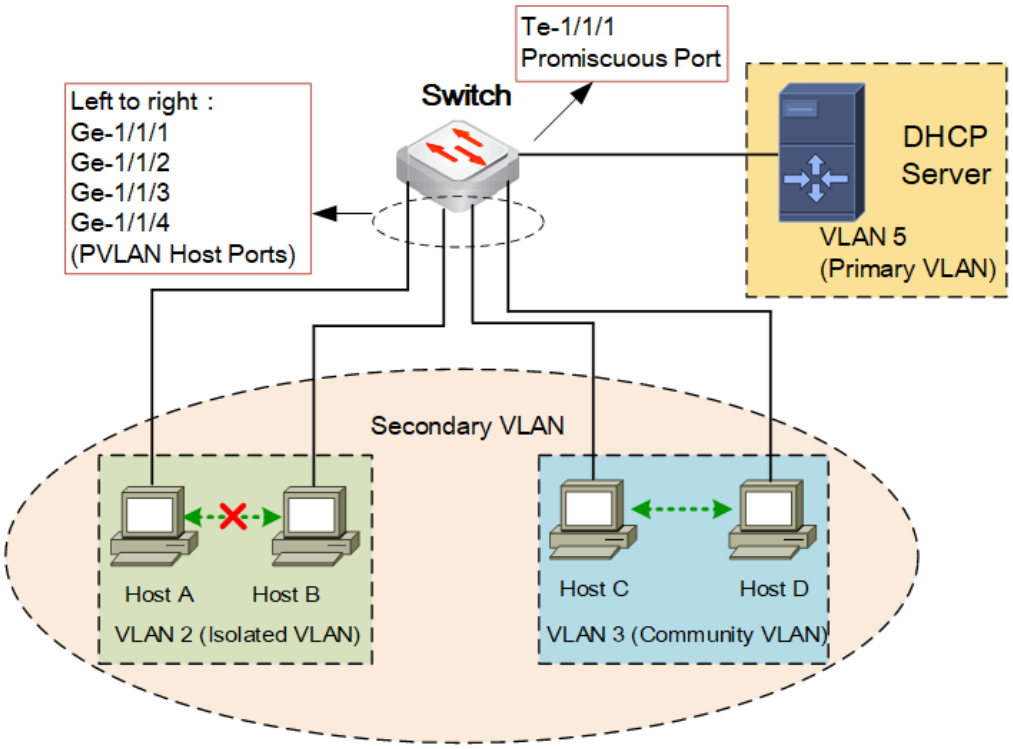
Host A and Host B cannot communicate with Host C and Host D at Layer 2.

Example for Configuring DHCP Snooping with PVLAN

- Networking Requirements
  - Figure 1. DHCP Snooping with PVLAN Configuration Example
- Procedure
- Verify the Configuration

Networking Requirements

Figure 1. DHCP Snooping with PVLAN Configuration Example



As shown in **Figure 1**, in the PVLAN topology, the Switch acts as a user gateway and forwards DHCP messages to DHCP server, so that DHCP clients Host A, Host B, Host C and Host D can apply for IP address lease and other related configuration information from the DHCP server. In order to provide better service to DHCP users, network administrators can configure DHCP Snooping to prevent DHCP attacks.

Complete the following configurations on the Switch:

- Configure PVLAN on the Switch. For details, please refer to 8.3.1 Example for Configuring PVLAN.
- Enable DHCP snooping on the primary VLAN, where the PVLAN pvlan-promiscuous port Te-1/1/1 connects to the DHCP server.
- Configure the PVLAN pvlan-promiscuous port Te-1/1/1 connecting to the DHCP server as a trust port.

Procedure

Step1 Create the secondary VLANs.

```
admin@XorPlus# set vlans vlan-id 2 private-vlan mode isolated
admin@XorPlus# set vlans vlan-id 3 private-vlan mode community
```

Step2 Create the primary VLAN.

```
admin@XorPlus# set vlans vlan-id 5 private-vlan mode primary
```

Step3 Associate the secondary VLAN with the primary VLAN.

```
admin@XorPlus# set vlans vlan-id 5 private-vlan association 2-3
```

Step4 Configure the ports connected to the hosts as the PVLAN host ports.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode pvlan-host
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode pvlan-host
```

Step5 Configure the port connected to the Server as the promiscuous port.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode pvlan-promiscuous
```

Step6 Add the host ports into the secondary VLAN and set the native VLAN of the host port as the secondary VLAN ID.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
```

Step7 Add the promiscuous port into the primary VLAN and set the native VLAN of the promiscuous port as the primary VLAN ID.

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 5
```

Step8 Configure DHCP snooping.

```
admin@XorPlus# set protocols dhcp snooping vlan 5 disable false
admin@XorPlus# set protocols dhcp snooping trust-port te-1/1/1
```

Step9 Commit the configurations.

```
admin@XorPlus# commit
```

Verify the Configuration

- You can use the **run show vlans private-vlan** command to view the PVLAN configuration information.

```
admin@Xorplus# run show vlans private-vlan
Primary   Secondary  Type            Tag         Interfaces
-------   ---------  -----------     --------    --------------------------
5                    primary         untagged    te-1/1/1
                                       tagged
          2          isolated        untagged    ge-1/1/1, ge-1/1/2
                                       tagged
          3          community       untagged    ge-1/1/3, ge-1/1/4
                                       tagged
```

- You can use the **run show vlans private-vlan type** command to view the PVLAN type information.

```
admin@Xorplus# run show vlans private-vlan type
Vlan Type
---- -----------
5    primary
2    isolated
3    community
```

- You can use the **run show dhcp snooping binding** command to view the DHCP snooping binding table.

```
admin@Xorplus# run show dhcp snooping binding
Total Snooping host count: 2
MAC Address        IP Address    Port       VLAN ID    Lease(sec)
-------------------------------------------------------------------------------------------
00:00:22:22:00:00  100.1.1.1     ge-1/1/1   101        599/600
00:00:33:33:00:00  100.1.1.2     ge-1/1/2   101        599/600
00:00:44:44:00:00  200.1.1.1     ge-1/1/3   102        599/600
00:00:55:55:00:00  200.1.1.2     ge-1/1/4   102        599/600
```

- DHCP clients can obtain IP addresses normally.

Voice VLAN Configuration Guide

- Principle of Voice VLAN
- Configuration Notes of Voice VLAN
- Configuring Voice VLAN
- Configuration Example of Voice VLAN

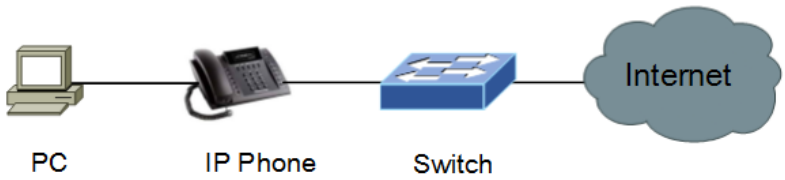
Principle of Voice VLAN

- Introduction
- OUI
- Auto and Manual Mode
  - Auto Mode
  - Manual Mode
- 802.1p Priority and DSCP Value
  - 802.1p Priority
  - DSCP Value
- Voice VLAN with LLDP
- Voice VLAN with LLDP Compliance CDP
- Data and Voice Packet Operation Process

Introduction

Voice over Internet Protocol (VoIP) is widely used today, but the performance of voice calls is greatly affected by the network quality. To make the quality of voice calls solid, you can use the voice VLAN technique which refers to a dedicated VLAN designed to handle the voice traffic. By configuring a voice VLAN on the switch to transmit voice data and setting QoS parameters of voice VLAN, we can make sure the voice data is given preference when congestion occurs.

Figure 1. Connecting a PC and an IP Phone to a Switch



As shown in Figure 1, a PC and an IP phone can be connected to the switch so that both data and voice services can be transmitted.

The switch can determine whether the data stream is a voice data stream according to the source MAC address field in the data packet of the ingress interface. The switch identifies the data packets as voice data when the source MAC address matches the system pre-configured Organizationally Unique Identifier (OUI).

OUI

OUI refers to the first 24 bits (binary) of the MAC address that can be used to represent a MAC address segment, which is a globally unique identifier assigned by the IEEE to different device vendors. Each device vendor then allocates another 24 bits to form a 48-bit MAC address. Voice packets sent by IP phones can be identified by its OUI.

In voice VLAN, the OUI is not necessarily 24 bits long which depends on the mask value. The OUI is the result of the AND operation between the MAC address and the mask value in the **set vlans voice-vlan mac-address mask** command.

The system uses three types of OUI: default OUI, user-defined OUI and learned OUI. The system has predefined seven OUIs, Table 1 lists all the default OUIs. User-defined OUI is configured by using **set vlans voice-vlan mac-address mask** command. Learned OUI is the OUI learned by the system if LLDP function or LLDP compliance with CDP function is enabled. Please note that in PICOS 2.11.4 and the later version , there is no default OUI.

Table 1. List of Default OUI

Default OUI	Description
00:01:e3:00:00:00	Siemens phone
00:03:6b:00:00:00	Cisco phone
00:04:0d:00:00:00	Avaya phone
00:60:b9:00:00:00	Philips/NEC phone
00:d0:1e:00:00:00	Pingtel phone
00:e0:75:00:00:00	Polycom phone
00:e0:bb:00:00:00	3com phone

Auto and Manual Mode

Auto and manual mode determine the way of the port when added to the voice VLAN.

Auto Mode

In auto mode, the system utilizes the voice packets or the protocol packets such as PICA8 supported LLDP, LLDP-MED and CDP sent by the IP phone to determine whether to add the port to voice VLAN. If the source MAC address of the packets matches the OUI address, the system will automatically add the ingress port of the voice packet into the voice VLAN, and implement the QoS priority to the voice VLAN. If the source MAC address of the packets matches no OUI address, the system will learn the source MAC address of the LLDP, LLDP-MED or CDP packet as the learned OUI and add the port to the voice VLAN.

If the IP phone supports one of the protocols of LLDP, LLDP-MED or CDP, please refer to section Voice VLAN with LLDP and Voice VLAN with LLDP Compliance CDP for details about the process of protocol packets.

You can set voice VLAN aging time of the device in auto mode. Until the aging time expires, if no voice packet is received from the ingress port, the system will delete the port from the voice VLAN after the aging time. The process of adding/deleting a port to the voice VLAN is implemented automatically by the voice VLAN feature.

Manual Mode

In manual mode, the ports are added to voice VLAN by manual configuration. If the source MAC address of the packets matches the OUI address, the system will implement the QoS priority of the voice VLAN. The process of adding/deleting a port to the voice VLAN is implemented manually by the administrator. This type of port is not affected by the aging time of the voice VLAN. When the aging time expires, the port will not be deleted from the voice VLAN.

802.1p Priority and DSCP Value

User can modify the 802.1p and DSCP priorities to meet the QoS requirement for voice traffic in the network. The default value of 802.1p and DSCP priorities of the voice VLAN feature are 6 and 46 respectively.

802.1p Priority

802.1p priority is the value of the priority field in the VLAN frame in IEEE 802.1Q standard, which contains the layer 2 priority to be used for the specified application type. This 3 bits field could specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004.

DSCP Value

Differentiated Services Code Point (DSCP) value is used to provide Diff-Serv (Differentiated Service) node behavior for the specified application type as defined in IETF RFC 2474. This 6 bits field may contain one of 64 code point values (0 through 63). The 6 bits Type of Service (TOS) field in the IPv4 data packet header is referred to as DSCP.

> **NOTE :**
>
> If the DSCP value of the voice VLAN is not set, the system does not modify the DSCP value carried by the packet by default.

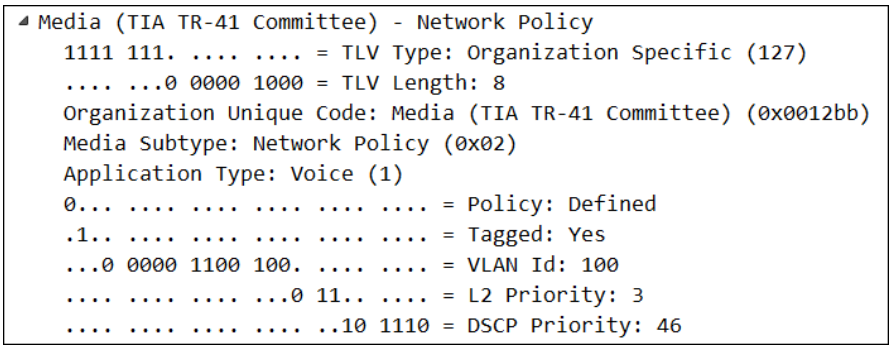
Voice VLAN with LLDP

Voice VLAN with LLDP means that PICA8 switch could learn OUI address from the source MAC address of the LLDP packet if LLDP is enabled between IP phone and PICA8 switch.

When receiving an LLDP packet, the system checks the Capabilities TLV in the LLDP packet. If the **telephone** value in both the **Capabilities** and **Enabled Capabilities** fields is **Capable**, the system considers the device connected to the switch as an IP phone. Afterwards, the system learns the source MAC address of the LLDP packet and saves it to the learned OUI table. The port is then added to the voice VLAN. You can view the learned OUI entries by using the **run show vlans voice-vlan oui** command and the **run show vlans** command to check whether the port has been added to the voice VLAN.

Besides the basic LLDP, the system also supports LLDP-MED for voice VLAN. Figure 2 is the content of the Network Policy TLV in LLDP-MED, mainly including the fields: Policy, Tagged, VLAN ID, L2 Priority and DSCP Priority. Network Policy TLV is used to exchange VLAN configuration between switches and terminal devices. A switch uses the TLV to advertise the local configuration of voice VLAN ID and QoS priority to an IP phone. Then the IP phone could totally decide what packets are sent according to the received information. “**run show lldp local_info detail**” and “**run show lldp neighbor detail**” commands can be used to view each field value of LLDP packet coming from the switch or the IP Phone.

Figure 2. Content of Network Policy TLV in LLDP-MED



Voice VLAN with LLDP Compliance CDP

When an IP phone in the network does not support LLDP but CDP protocol, a proprietary link discovery protocol of Cisco, you can enable LLDP compliance CDP function in order to be compatible with CDP protocol and guarantee that the switch can discover and identify this type of neighbor node. You have to enable LLDP function before using LLDP compliance CDP function.

Data and Voice Packet Operation Process

Data packets and voice packets may arrive at the same port. Even if both traffics are untagged packets, we could use the ingress ACLs based on OUI to separate these two types of packets. Any untagged VoIP traffic will be tagged with voice VLAN ID and the 802.1P priority and DSCP value will be modified when transmitted to the egress port if it successfully matches an ingress ACL. As a result, we can separate these two types of untagged traffic into two different VLANs and both data packets and voice packets can be transmitted in parallel.

Configuration Notes of Voice VLAN

When configuring Voice VLAN on a device, pay attention to the following points:

- Voice VLAN could not be configured as PVID or VLAN members on a port, in other words, PVID or VLAN members on a port could not be configured as voice VLAN.
- Voice VLAN could not be configured on the LAG interface.
- Voice VLAN MUST be configured on the port with trunk port-mode.
- Only one VLAN can be configured as voice VLAN on an interface at a time.
- The system supports a maximum of 10 OUIs, including the default 7 OUIs. In PICOS 2.11.4 and the later version, there is no default OUI, the user is allowed to configure a maximum of 10 OUIs.
- A chassis switch supports a maximum of 4 voice VLANs.

Configuring Voice VLAN

Procedure

Step1 Configure VLAN, configure the port mode to **trunk**.

a) Create a VLAN.

set vlans vlan-id <*vlan-id*>

b) Configure the port mode to **trunk**.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode <***port-mode*>

Step2 Configure an interface into voice VLAN.

set interface gigabit-ethernet <*interface-name*> **voice-vlan vlan-id <***vlan-id*>

Step3 Configure the mode for how an interface is added to a voice VLAN.

set interface gigabit-ethernet <*interface-name*> **voice-vlan mode** {**auto | manual**}

Step4 Configure the tagged mode for the outgoing packet of a voice VLAN interface.

set interface gigabit-ethernet <*interface-name*> **voice-vlan tagged mode** <**tag | untag | auto**>

Step5 Configure the aging time for voice VLAN.

set vlans voice-vlan aging <*aging-time*>

Step6 Configure an OUI for the voice VLAN.

set vlans voice-vlan mac-address <*mac-address*> **mask** <*oui-mask*>

The system supports a maximum of 10 OUIs, including the default 7 OUIs. After PICOS version 2.11.4, there is no default OUI, the user is allowed to configure a maximum of 10 OUIs.

Step7 (Optional) Configure description information for the OUI address.

set vlans voice-vlan mac-address <*mac-address*> **description** <*text*>

Step8 Configure the 802.1p priority and DSCP value for a voice VLAN.

set vlans voice-vlan local-priority <*priority-value*>

set vlans voice-vlan dscp <*dscp-value*>

Step9 Enable LLDP function to support IP phone of LLDP, LLDP-MED and CDP.

set protocols lldp enable <**true | false**>

Step10 Enable LLDP compliance with CDP to support IP phone of CDP.

a) Enable global LLDP compliance with CDP.

set protocols lldp compliance cdp <**true | false**>

b) Enable interface-based LLDP compliance with CDP.

set protocols lldp interface <*interface-name*> **compliance cdp** <**true** | **false**>

NOTE:

- To enable LLDP compliance with CDP on a specific interface, you need to enable both the global and interface-based LLDP compliance with CDP functions.
- To avoid unnecessary trouble, you should only configure CDP compliance on access port intended for VoIP phones, but do not configure CDP on other interfaces.

Configuration Example of Voice VLAN

Procedure

Step1 Configure the VLAN, configure port mode to **trunk**.

```
admin@XorPlus# set vlans vlan-id 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
```

Step2 Configure an interface into voice VLAN.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 voice-vlan vlan-id 10
```

Step3 Configure the mode for how an interface is added to a voice VLAN.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 voice-vlan mode manual
```

Step4 Configure the tagged mode for the outgoing packet of a voice VLAN interface.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 voice-vlan tagged mode tag
```

Step5 Configure the aging time for voice VLAN.

```
admin@XorPlus# set vlans voice-vlan aging 600
```

Step6 Configure an OUI for the voice VLAN.

```
admin@XorPlus# set vlans voice-vlan mac-address 00:11:11:00:00:01 mask ff:ff:ff:00:00:00
```

Step7 (Optional) Configure description information for the OUI address.

```
admin@Xorplus# set vlans voice-vlan mac-address 00:11:11:00:00:01 description CompanyPhone
```

Step8 Configure the 802.1p priority and DSCP priority for a voice VLAN.

```
admin@XorPlus# set vlans voice-vlan local-priority 6
admin@XorPlus# set vlans voice-vlan dscp 63
```

Step9 Enable LLDP function to support IP phone of LLDP, LLDP-MED and CDP.

```
admin@XorPlus# set protocols lldp enable true
```

Step10 Enable LLDP compliance with CDP to support IP phone of CDP.

a) Enable global LLDP compliance with CDP.

```
admin@XorPlus# set protocols lldp compliance cdp true
```

b) Enable interface-based LLDP compliance with CDP.

```
admin@XorPlus# set protocols lldp interface ge-1/1/1 compliance cdp true
```

NOTE:

- To enable LLDP compliance with CDP on a specific interface, you need to enable both the global and interface-based LLDP compliance with CDP functions.
- To avoid unnecessary trouble, you should only configure CDP compliance on access port intended for VoIP phones, but do not configure CDP on other interfaces.

Verify the Configuration

- You can use the **run show vlans voice-vlan oui** command to view the OUI addresses of voice VLAN, including default OUI, user-configured OUI and learned OUI.

```
admin@XorPlus# run show vlans voice-vlan oui
Oui_Address          Mask                 Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0       Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0       Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0       Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0       Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0       Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0       Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0       3com phone
00:11:11:00:00:01 ff:ff:ff:0:0:0      CompanyPhone
Learned_Oui_Address     Mask
22:22:22:22:11:11    ff:ff:ff:ff:ff:ff
22:22:22:22:22:22    ff:ff:ff:ff:ff:ff
22:22:22:22:33:33    ff:ff:ff:ff:ff:ff
22:22:22:22:44:44    ff:ff:ff:ff:ff:ff
```

- You can use the **run show vlans voice-vlan** command to view the configuration information of a voice VLAN.

```
admin@XorPlus# run show vlans voice-vlan vlan-id 10
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:63
Voice Vlan aging time:600 minutes
Current voice vlan enabled port mode:
Port       Mode      Tagged    Mac_Address     Status
-------------------------------------------------------------------------
ge-1/1/1    manual      true    00:11:11:00:00:01   Working
```

- You can use the **run show vlans vlan-id** <*vlan-id*> command to check whether the port has been added to the voice VLAN.

```
admin@XorPlus# run show vlans vlan-id 10
VLAN ID: 10
VLAN Name: default
Description: CompanyPhone
vlan-interface:
Routed-interface:
Number of member ports: 1
Untagged port: None
Tagged port: ge-1/1/1
```

- You can use the **run show lldp neighbor** <*interface-name*> **detail** command to view the LLDP information of neighbor device.

```
admin@XorPlus# run show lldp neighbor ge-1/1/1 detail
Local Port: ge-1/1/1
LLDP info:
Time To Live: 180
 Chassis Id: 192.1.1.1
 Port ID: 189C5DB7E4F4:P1
 Port Description: SW PORT
 System Name: SEP189C5DB7E4F4
 System Description: Cisco IP Phone 7965G,V14,
 System Capability: Bridge, Telephone
 Management Address:
 Default VLAN ID: 0
 Auto Negotiation: Supported, Enabled
 Physical media capabilities: FDX_S_Pause, FDX_B_Pause, 1000base_XFD, 1000base_T
 Media Attachment Unit type: 1000base_T_Full_Duplex
 +Med capabilities: Capabilities, Network Policy, Extended Power via MDI-PD, Inventory
 Med device type: Endpoint Class III
 +MED Network Policy
 Application Type: Voice
 Policy Flags: Known Policy
 Vlan ID: 10
```

```
L2 Priority: 6
DSCP Value: 63
+MED Network Policy
Application Type: Voice Signaling
Policy Flags: Known Policy
Vlan ID: 10
L2 Priority: 0
DSCP Value: 0
+MED Extended Power via MDI
Power Type: PD device
Power Source: Unknown
Power Priority: Unknown
Power Value: 12.0 watts
+MED Hardware revision: 14
+MED Firmware revision: tnp65.9-3-1-CR17.bin
+MED Software revision:
+MED Serial number: FCH174499U2
+MED Manufacturer: Cisco Systems, Inc.
+MED Model name: CP-7965G
+MED Asset ID:
```

- You can use the **run show lldp local_info**<*interface-name*> **detail** command to view the LLDP information of local device.

```
admin@XorPlus# run show lldp local_info ge-1/1/1 detail
LLDP Local configuration details
Chassis ID: 70:72:cf:fd:8f:21
System name: XorPlus
System description: PICA8 Inc., Model as4610_30p, PicOS 2.9.1
Interface     LLDP    State
---------- --------- ---------
ge-1/1/1    Enable    tx_rx

+Med capabilities: Capabilities, Network Policy, Extended Power via MDI-PD, Inventory
Med device type: Network Connectivity
+MED Network Policy
Application Type: Voice
Policy Flags: Unknown Policy
Vlan ID: 10
L2 Priority: 6
DSCP Value: 63
+MED Network Policy
Application Type: Voice Signaling
Policy Flags: Unknown Policy
Vlan ID: 10
L2 Priority: 0
DSCP Value: 0
+MED Extended Power via MDI
Power Type: PSE device
Power Source: Primary Power Source
Power Priority: Unknown
Power Value: 0.0 watts
+MED Hardware revision: N/A
+MED Firmware revision: 2.9.1/ac36038
+MED Software revision: 2.9.1/ac36038
+MED Serial number: AF10029779
+MED Manufacturer: Edgecore
+MED Model name: as4610_30p
+MED Asset ID: N/A
```

Link Aggregation Configuration

- Static Link Aggregation (LAG) Configuration
- Link Aggregation Control Protocol (LACP) Configuration
- LAG Hashing Configuration
  - LAG Hashing Configuration and Example
  - LAG Hash Mapping
  - Resilient LAG Hashing Configuration and Example
- LACP Fallback
- Configuring LACP Fast Rate
- LAG Specification of Different Platforms

Static Link Aggregation (LAG) Configuration

- Both static and LACP LAGs can support the hashing of traffic using the Src/Dst MAC address, the Src/DstIP address, and Layer 4 port information.
- If all member ports of a LAN are link-down, the LAG will be link-down. The LAG will become link-up when at least one member port is link-up.
- The logical function and configuration of LAGs are same as those of a physical port.

Configuring Static LAGs

The name of the LAG interface is a string in the format of **ae***x*, where x is an integer ranging from 1 to 4094.

> The maximum LAGs per switch is limited by the interface capacity.

```
admin@XorPlus# set interface aggregate-ethernet ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 ether-options 802.3ad ae1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Displaying Static LAG Information

```
admin@XorPlus# run show interface aggregate-ethernet ae1
Physical interface: ae1, Enabled, Physical link is Up
Interface index: 53
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Current address: c8:0a:a9:9e:14:9f, Hardware address: c8:0a:a9:9e:14:9f
Traffic statistics:
Input Packets.............................176
Output Packets............................16
Input Octets..............................12888
Output Octets............................1594
Aggregated link protocol: STATIC
Members Status Port Speed
--------- -------- ----------
ge-1/1/1 Down Auto
ge-1/1/2 Down Auto
ge-1/1/3 Up Auto
ge-1/1/4 Up Auto
```

Link Aggregation Control Protocol (LACP) Configuration

LACP (802.3ad) provides the dynamic link aggregation function.

The LACPDU includes the LACP system priority, the system MAC, the port priority, and I.D. The port, included in the LACP LAG, will transmit the LACPDU to its neighbors.

The configuration of the LACP LAG is similar to that of the static LAG.

The **min-selected-port** label denotes that the LAG is up only when no fewer than the defined number of ports are up. Below, our defined number is 4.

Configuring LACP LAGs

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options min-selected-port 4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 ether-options 802.3ad ae1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Displaying LACP LAG Information

```
admin@XorPlus# run show interface aggregate-ethernet ae1
Physical interface: ae1, Enabled, Physical link is Down
Interface index: 53
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Current address: 60:eb:69:d2:9c:d7, Hardware address: 60:eb:69:d2:9c:d7
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Output Packets............................0
Input Octets..............................0
Output Octets............................0
Aggregated link protocol: LACP
Minimum number of selected ports: 4
Members Status Port Speed
--------- ---------- ----------
ge-1/1/1 up(active) Auto
ge-1/1/2 up(active) Auto
ge-1/1/3 up(active) Auto
ge-1/1/4 up(active) Auto
```

LAG Hashing Configuration

The IEEE 802.3ad link aggregation protocol groups multiple Ethernet interfaces and forms a single link layer interface known as LAG (link aggregation group). Traffic is balanced across the member links in the LAG to make use of all available bandwidth. The balancing is done by the LAG hashing algorithm. The LAG hashing algorithm determines the member link to be used for an incoming frame on the basis of certain values in the frame header.

- LAG Hashing Configuration and Example
- LAG Hash Mapping
- Resilient LAG Hashing Configuration and Example

LAG Hashing Configuration and Example

This example configures the LAG hash mapping mode as **ethernet-destination-only**.

Configuration:

```
set interface aggregate-ethernet ae1 hash-mapping mode ethernet-destination-only
```

Examples:

Configure one LAG with three ports.

```
set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae10
```

Examples:

Configure the LAG hash mapping mode as **ethernet-destination-only**.

```
set interface aggregate-ethernet ae10 hash-mapping mode ethernet-destination-only
```

LAG Hash Mapping

User can configure the LAG hash mapping field according to the requirement.

Configure one LAG with three ports.

```
set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae10
```

Configure the LAG hash mapping mode as **ethernet-destination-only**.

```
set interface aggregate-ethernet ae10 hash-mapping mode ethernet-destination-only
```

Configure the LAG hash mapping field.

```
set interface aggregate-balancing hash-mapping field ethernet-destination-address disable false
set interface aggregate-balancing hash-mapping field ethernet-source-address disable false
```

Resilient LAG Hashing Configuration and Example

Configure the LAG hashing mode as **advanced-resilient**. By default, the hash-mapping field is **disable false all**.

Without resilient mode, each traffic flow (the flow definition depends on the hash-mapping configuration) is load balanced on one port of the LAG. This distribution is done via a hashing algorithm. If a port on this LAG is added or removed (link up/down), the hash will change all flows to be re-distributed on the remaining ports. It is typically not important if the device on the other side of the LAG is a router or a switch but could be important if the LAG is sending traffic to equipment (like a cluster of servers) that handles traffic differently on each port (for example, distributing http sessions on multiple servers).

In resilient mode, a removed link does not trigger the redistribution of traffic on the remaining ports. Only the traffic from the removed port will be distributed to the remaining ports. An added link does not trigger redistribution of traffic on the remaining ports. The added link will share the traffic on the remaining ports.

> ⚠ Currently, only switch models of Trident, Trident II, Trident II+, and Trident3-X5 support the resilient LAG hashing feature.

Configuration:

```
set interface aggregate-ethernet ae10 hash-mapping mode advanced-resilient
```

Examples:

Configure one lag with three ports

```
set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae10
set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae10
```

Configure the lag hash mode advanced-resilient

```
set interface aggregate-ethernet ae10 hash-mapping mode advanced-resilient
```

Configure the hash-mapping field

```
  set interface aggregate-balancing hash-mapping field ip-destination disable false
  set interface aggregate-balancing hash-mapping field ip-source disable false
```

LACP Fallback

- Overview
  - Application Scenarios
  - Timer
  - Port Election
- Configuring LACP Fallback
  - Prerequisite Configurations
  - Enable LACP Fallback
- Configuration Example
  - Procedure

NOTE:
Some PXE servers cannot send DHCP discover messages continuously, which may result in failure to obtain IP addresses, thus affecting device communication.

When such an issue is encountered, you can try the following two methods to solve the problem.

1. Set the LACP fallback timer to 0 by using the following command.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback timeout 0
admin@Xorplus# commit
```

By default, the LACP fallback timer is 10 seconds. After LACP configurations are finished, you have to wait for the timer to expire before the LACP fallback port can forward packets.

2. Disable spanning tree function by using the following command.

```
admin@Xorplus# set protocols spanning-tree enable false
admin@Xorplus# commit
```

Spanning tree is enabled by default, which will wait 9 seconds before the port can forward packets.

However, if you do not want to disable spanning tree, you can use the following command to configure *manual-forwarding* on the LAG port, so that messages can be forwarded immediately after the LAG port is up.

```
admin@Xorplus# set protocols spanning-tree mstp interface ae1 manual-forwarding true
admin@Xorplus# commit
```

Overview

The LACP fallback feature sets the LACP LAG port to fallback mode and brings up one of the member ports to the active (up) state before any LACP PDUs is received by the LAG port. The fallback mode will not exit until one LACP PDU is received by any one of the member ports from the peer device.

Application Scenarios

This feature is useful for scenarios where the peer device is a Preboot Execution Environment (PXE) booting client and connected through a LAG interface on Pica8 switch. With LACP fallback feature enabled on Pica8 switch, a PXE booting client can complete the PXE booting process and system configurations by connecting to the DHCP server/TFTP server through one of the active LAG member ports on Pica8 switch.

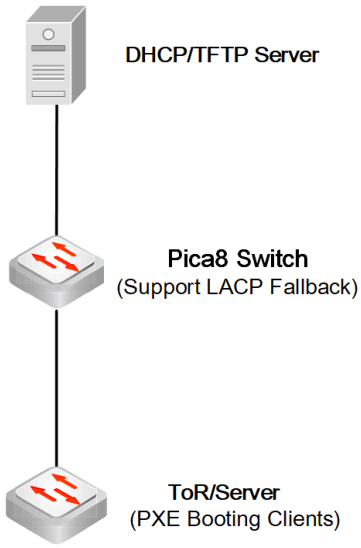
The following sections describe in detail the application scenarios of LACP Fallback in both non-MLAG and MLAG networks.

Non-MLAG Networks

As shown in Figure 1, in Non-MLAG networks, where the peer device connected to the Pica8 Switch is a Server or ToR through an LACP LAG port on Pica8 Switch.

Such Server and ToR are PXE booting clients, which cannot send and process LACP messages during the PXE phase. This causes the connected LAG port on Pica8 Switch to be inactive and unable to communicate with the PXE booting clients. These clients need the link to be active so that they can reach the DHCP or TFTP server to get the necessary installation files.

Figure 1. LACP Fallback Applied in Non-MLAG Networks

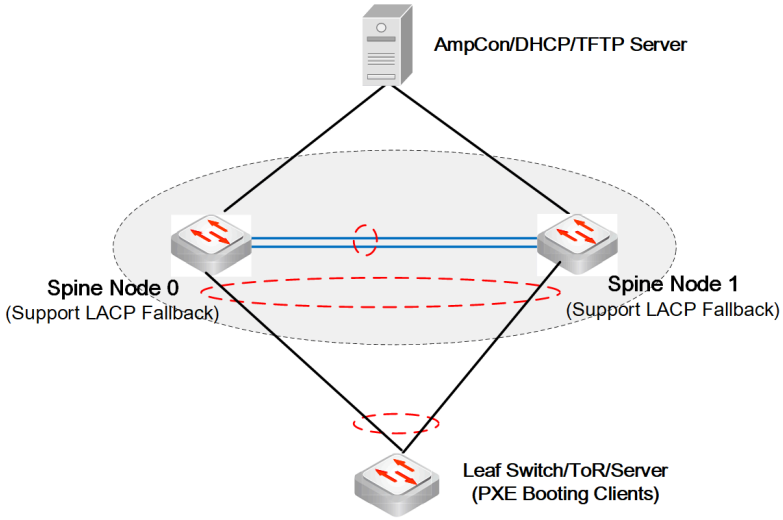


With LACP fallback feature, a Pica8 Switch will allow the system to bring up the LAG (before receiving any LACP PDUs from the PXE booting clients) and keeps one of the member ports active until receiving an LACP PDU by one of the member ports from the peer. This allows the PXE booting clients to establish a connection, download its boot image and then continue the boot process. When the boot process is complete, the server will fully support to form an LACP LAG.

MLAG Networks

As shown in Figure 2, in MLAG networks or an AmpCon application scenario, LACP Fallback can be configured on the spine switches. The newly deployed Leaf switch/ToR/Server in bare metal state with no NOS installed, will not be able to send and process LACP messages during the PXE phase. This causes the LAG port connected on the Spine switches to be inactive and hence making it impossible for the Leaf switch/ToR/Server to reach the AmpCon/DHCP/TFTP server to complete the system installation.

Figure 2. LACP Fallback Applied in MLAG Networks



With LACP fallback feature, Spine switches allow the system to bring up the LAG (before receiving any LACP PDUs from the Leaf switch/ToR/Server) and keeps one of the member ports active until receiving an LACP PDU on any one of the member ports from the Leaf switch/ToR/Server. This allows the newly installed Leaf switches/ToR/Server to establish a connection, reaching the AmpCon server to get provisioned.

NOTEs:

- Upon receiving the first LACP PDU, the system will exit the fallback mode. The system will not start the LACP Fallback process again afterwards, even if no LACP PDUs are received from the peer later for an LACP fallback timer. But there are some special cases, that is, all LAG member ports are down or the peer device is replaced after the system has exited from the LACP fallback mode. Only in these special cases, the LACP Fallback process can be started again.
- For MLAG environment, the LACP fallback configurations should be consistent on MLAG peers.

Timer

The switch starts LACP fallback timer when LACP configurations are finished and LACP fallback is enabled on the switch. If no LACP PDUs are received from the peer device on any of the member ports of the LAG when this timer expires, the switch will set the LAG to fallback mode and bring up one member port to active (up) state.

The switch will not exit LACP fallback mode until it receives an LACP PDU from the peer device.

Use the following command to configure the LACP fallback timer. The default value is 10 seconds.

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback timeout** <*timer*>

Port Election

Since only one member port of the LAG can be chosen as the active port, the port election rules are:

- The port with *lowest LACP port priority value* will be chosen as the active port.
- If LACP port priorities are the same, port with *lowest port index* will be chosen as the active port.

The following command can be used to set priority of the LACP member port:

set protocols lacp interface <*physical-port*> **priority** <*priority-value*>

For non-MLAG environment, the port election rule is as described above.

For MLAG environment, port election is first performed on each MLAG peer device. Then the elected ports information is exchanged between MLAG peers. And finally, an active port is elected from these two ports according to the port election rules described above.

LACP Fallback supports fallback port preemption. A port with a higher priority can always preempt the active fallback port as the new active fallback port. During LACP fallback mode, when a non-fallback port is configured with a higher priority, the system will perform port re-election, as a result, the higher priority port will replace the elected port as the active port.

Configuring LACP Fallback

Prerequisite Configurations

1. Create a LAG interface.
2. Add member ports to the LAG interface.
3. Enable LACP protocol on the LAG interface.

> **NOTEs:**
> LACP fallback can only be applied on the LACP LAG interface, but not on a static LAG.

Enable LACP Fallback

- Enable LACP fallback.

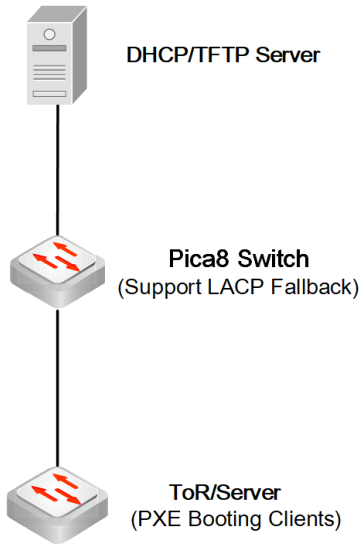
set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback enable** <**true | false**>

- (Optional) Configure LACP fallback timer. The default value is 10 seconds.

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback timeout** <*timer*>

Configuration Example

As shown in the following figure, Pica8 Switch and the PXE Booting Clients (ToR or Server) are connected through an LACP LAG interface. You can enable LACP fallback function on Pica8 Switch, which will allow the PXE Booting Client to connect to the DHCP/TFTP Server through one active port on Pica8 Switch during the PXE phase.



Procedure

Step 1 Create a LAG interface **ae1**, add physical ports and enable LACP protocol on the LAG.

```
admin@XorPlus# set interface aggregate-ethernet ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae1
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
```

Step 2 Enable LACP fallback on LAG interface **ae1**.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback enable true
```

Step 3 Commit the configurations.

```
admin@XorPlus# commit
```

Step 4 Verify the configurations.

Run the command **run show interface aggregate-ethernet** <*lag-interface*> to display configuration information and status of the LAG interface, "*Fallback: Enabled*" shows that LACP fallback is enabled.

```
admin@XorPlus# run show interface aggregate-ethernet ae1
Physical interface: ae1, Enabled, error-discard False, Physical link is Up
Interface index: 80, Mac Learning Disabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1518, Speed: 1Gb/s, Duplex: Auto
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Disabled
Interface flags: SNMP-Traps Internal: 0x0
Current address: e0:07:1b:c9:20:9b, Hardware address: e0:07:1b:c9:20:9b
Traffic statistics:
  5 sec input rate 952 bits/sec, 1 packets/sec
  5 sec output rate 624 bits/sec, 1 packets/sec
  Input Packets.....................25877
  Output Packets....................29275
  Input Octets......................2445697
  Output Octets.....................2509890
Aggregated link protocol: LACP
Fallback: Enabled
Minimum number of selected ports: 0
  Members        Status          Port Speed
  ---------      ----------      ----------
  ge-1/1/1      Up(active)      1Gb/s
  ge-1/1/2      Up(active)      1Gb/s
  ge-1/1/3      Up(active)      1Gb/s
```

LAG Specification of Different Platforms

The following specifications supportd by LAG are model dependent, we have collected them in page Collection of Feature Specification of Different Platforms:

- the maximum number of LAGs supported by a switch
- the maximum number of member ports supported by a switch

Symmetric Hash for LAG Configuration Example

Symmetric Hash support for LAG. Symmetric hash need the hashing field must be symmetric. For example, packet 1 and packet 2 are symmetric in table 1 and table 2 as below, and then packet 1 and packet2 will go out from the same physical port. Now Our symmetric Hash use IP layer and L4 field to hash when packets are transmitted on LAG port. Only matching symmetric condition, two packets can be transmitted on the same member port of LAG interface.

IP Packet	Source IP Address	Destination IP Address
Packet1	10.1.1.1	20.1.1.1
Packet2	20.1.1.1	10.1.1.1

Table 1.

Layer 4 Packet	Source IP Address	Destination IP Address	Source Port Number	Destination Port Number
Packet1	10.1.1.1	20.1.1.1	100	200
Packet2	20.1.1.1	10.1.1.1	200	100

Table 2.

Symmetric Hash field as below:

1. ip-source
2. ip-destination
3. port-source
4. port-destination

By default, Enable hash field on LAG interface:

1. ingress-interface
2. ethernet-source-address
3. ethernet-destination-address
4. ethernet-type
5. vlan
6. ip-protocol
7. ip-source
8. ip-destination
9. port-source
10. port-destination

> LAG interface enables 10 fields to hash more than symmetric hashing 4 fields in the default case. So if to need symmetric hash work on lag interface，please it is best to disable the following field：
>
> 1. ingress-interface
> 2. ethernet-source-address
> 3. ethernet-destination-address
> 4. ethernet-type
> 5. vlan
> 6. ip protocol

> Symmetric hashing is supported on Helix4 **,** Trident2, Trident2+, Trident3 and Tomahawk platform switches.

LAG Hashing Configuration

```
set interface aggregate-ethernet ae1 hash-mapping mode advanced
set interface aggregate-balancing hash-mapping symmetric true
```

LAG Hashing Examples:

configure one lag with three ports:

```
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 199
set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 299
set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae1
set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad ae1
set interface gigabit-ethernet te-1/1/4 ether-options 802.3ad ae1
set protocols static route 100.100.100.0/24 next-hop 182.168.1.100
set protocols static route 172.168.1.0/24 next-hop 182.168.1.100
```

```
set l3-interface vlan-interface vlan199 address 172.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan299 address 182.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan399 address 100.100.100.1 prefix-length 24
set vlans vlan-id 199 l3-interface vlan199
set vlans vlan-id 299 l3-interface vlan299
set vlans vlan-id 399 l3-interface vlan399
```

Configure the symmetric hash true

```
set interface aggregate-ethernet ae1 hash-mapping mode advanced
set interface aggregate-balancing hash-mapping symmetric true
set interface aggregate-balancing hash-mapping field ingress-interface disable true
set interface aggregate-balancing hash-mapping field ethernet-source-address disable true
set interface aggregate-balancing hash-mapping field ethernet-destination-address disable true
set interface aggregate-balancing hash-mapping field ethernet-type disable true
set interface aggregate-balancing hash-mapping field vlan disable true
set interface aggregate-balancing hash-mapping field ip-protocol disable true
```

LLDP Configuration (Link Layer Discovery Protocol)

LLDP is a standard link-layer discovery protocol which can broadcast its capability, IP address, ID, and interface name as TLVs (Type/Length/Value) in LLDP PDUs (Link Layer Discovery Protocol Data Units).

An LLDP PDU includes 4 basic TLVs and several optional TLVs.

Basic TLVs include the Chassis ID, Port ID, TTL and End TLVs.

In L2/L3, you can select the following optional TLVs:

TLV Name	Description
mac-phy-cfg	MAC address of the system
management-address	Management IP address of the system
port-description	The port description of system
port-vlan	The VLAN ID of the port
system-capabilities	System capability (e.g. switching, routing)
system-description	System description
system-name	System name

Configuring the LLDP Mode

LLDP supports 4 modes: TxRx, Tx_only, Rx_only, and Disabled. By default, LLDP is disabled.

In TxRx mode, the system transmits *and* receives LLDPDUs. In Tx_only, the system only transmits LLDPDUs. In Rx_only, the system only receives LLDPDUs. In Disabled, the system will not transmit or receive any LLDPDUs.

After enabling LLDP, each interface will be in tx_rx mode by default.

You can configure the system as shown below:

Selecting Optional TLVs

```
admin@XorPlus# set protocols lldp tlv-select mac-phy-cfg true
admin@XorPlus# set protocols lldp tlv-select management-address true
admin@XorPlus# set protocols lldp tlv-select port-description true
admin@XorPlus# set protocols lldp tlv-select system-capabilities true
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Displaying LLDP Information

```
admin@XorPlus# show protocols lldp
```

```
    enable: true
>   interface "xe-1/1/3" {
>       compliance {
>           cdp: true
>       }
>   }
>   tlv-select {
>   }
admin@XorPlus# run show lldp neighbor all detail
Local Port: te-1/1/1
LLDP info:
------------------------------------------------------------------------------
  Time To Live: 106
  Chassis Id: 68:21:5F:7F:10:C6
  Port ID: te-1/1/1
  Port Description: te-1/1/1
  System Name: PICOS
  System Description: Pica8, Inc.,AS5835_54T, PICOS 4.3.2/9b1219e332
  System Capability: B, RBridge, Router
  System Enabled Capability: Bridge, Router
  Management Address: 10.10.51.12
  Default VLAN ID: 1
  Auto Negotiation: Supported, Enabled
  Physical media capabilities: Others, 10base_T, 100base_TX, 100base_TXFD, 1000base_T, 1000base_TFD
  Media Attachment Unit type: 1000base_T_Full_Duplex
  802.3 Power via MDI :Not available


LLDP MED is not Enabled.


Total entries displayed: 1
```

Configuring Other Parameters

You can configure other parameters, such as advertisement-interval, hold-time-multiplier, reinit-delay, and transmit-delay, in a similar manner.

LLDP MED Configuration

In LLDP-MED protocol, it provides extra Organizationally Specific TLVs. The TLVs lists that Pica8 switch support are as follows :

M Mandatory for this TLV to be included in all outgoing LLDP-MED LLDPDUs,

C Conditionally required, mandatory for this TLV to be included in outgoing LLDP-MED LLDPDUs under the described conditions,

LLDP-MED TLV Subtype	TLV Name	LLDPDU Usage
1	LLDP-MED Capabilities	M
2	Network Policy	C1
3	Location Identification	C1
4	Extended Power-via-MDI	C2

Note 1: Transmission of these mandatory TLVs only applies if the associated TLV data contents have been administratively configured and apply on a given port.

Note 2: Extended Power-via-MDI TLV is mandatory for IEEE 802.3af compliant PSE Network Connectivity Devices. This TLV is not applicable for non-PoE capable ports, and should not be included in outgoing LLDP-MED LLDPDUs on such ports.

Basic Configuration:

Enable LLDP

```
set protocols lldp enable true
```

Configure lldp med tlvs

- basiclly these tlvs are selected by default:

```
set protocols lldp med-tlv-select inventory-management true/false
set protocols lldp med-tlv-select network-policy true/false
set protocols lldp med-tlv-select extended-power-via-mdi true/false
```

- Configure the lldp med fast start repeat count:
- The LLDP-MED fast start repeat count specifies the number of LLDP packets that will be sent during the LLDP-MED fast start period.

```
set protocols lldp med-fast-start-repeat-count 5
```

The LLDP MED function will only be active by receiving lldp med packets.

Show the med working status:

```
admin@XorPlus# run show lldp detail
LLDP: Enable
Advertisement interval: 30
Re-initialization Delay: 2
Transmit Delay: 2
Hold timer: 120
LLDP-MED fast start repeat count: 5
Selected TLVs:
 port_description
 system_name
 system_description
 system_capabilities
 management_address
 port_vlan_id
 mac_phy
Selected MED TLVs:
 inventory management
 network_policy
 extended power via mdi
```

Show the med information of neighbor device:

```
admin@XorPlus# run show lldp neighbor ge-1/1/1 detail
Local Port: ge-1/1/1
LLDP info:
 Time To Live: 180
 Chassis Id: 192.1.1.1
 Port ID: 189C5DB7E4F4:P1
 Port Description: SW PORT
 System Name: SEP189C5DB7E4F4
 System Description: Cisco IP Phone 7965G,V14,
 System Capability: Bridge, Telephone
 Management Address:
 Default VLAN ID: 0
 Auto Negotiation: Supported, Enabled
 Physical media capabilities: FDX_S_Pause, FDX_B_Pause, 1000base_XFD, 1000base_T
 Media Attachment Unit type: 1000base_T_Full_Duplex
```

```
 +Med capabilities: Capabilities, Network Policy, Extended Power via MDI-PD, Inventory
 Med device type: Endpoint Class III
 +MED Network Policy
 Application Type: Voice
 Policy Flags: Known Policy
 Vlan ID: 4095
 L2 Priority: 5
 DSCP Value: 46
 +MED Network Policy
 Application Type: Voice Signaling
 Policy Flags: Known Policy
 Vlan ID: 4095
 L2 Priority: 0
 DSCP Value: 0
 +MED Extended Power via MDI
 Power Type: PD device
 Power Source: Unknown
 Power Priority: Unknown
 Power Value: 12.0 watts
 +MED Hardware revision: 14
 +MED Firmware revision: tnp65.9-3-1-CR17.bin
 +MED Software revision:
 +MED Serial number: FCH174499U2
 +MED Manufacturer: Cisco Systems, Inc.
 +MED Model name: CP-7965G
 +MED Asset ID:
```

Show the med information of local device:

```
admin@XorPlus# run show lldp local_info ge-1/1/1 detail
LLDP Local configuration details
Chassis ID: 70:72:cf:fd:8f:21
System name: XorPlus
System description: PICA8 Inc., Model as4610_30p, PicOS 2.9.1
Interface LLDP State
---------- --------- ---------
ge-1/1/1 Enable tx_rx

 +Med capabilities: Capabilities, Network Policy, Extended Power via MDI-PD, Inventory
 Med device type: Network Connectivity
 +MED Network Policy
 Application Type: Voice
 Policy Flags: Unknown Policy
 Vlan ID: 0
 L2 Priority: 6
 DSCP Value: 46
 +MED Network Policy
 Application Type: Voice Signaling
 Policy Flags: Unknown Policy
 Vlan ID: 0
 L2 Priority: 0
 DSCP Value: 0
 +MED Extended Power via MDI
 Power Type: PSE device
 Power Source: Primary Power Source
 Power Priority: Unknown
 Power Value: 0.0 watts
 +MED Hardware revision: N/A
 +MED Firmware revision: 2.9.1/ac36038
 +MED Software revision: 2.9.1/ac36038
 +MED Serial number: AF10029779
 +MED Manufacturer: Edgecore
 +MED Model name: as4610_30p
 +MED Asset ID: N/A
```

MSTP Configuration

802.1D, 802.1w, and 802.1s are spanning tree protocols that can avoid the loop in Layer2. You can configure the parameters of MSTP, including bridge-priority, forward-delay, max-age, and hello-time interval.

NOTE:

- A chassis switch supports a maximum of 16 MST instances.
- Once the spanning tree protocol is enabled on the network, the port starts to perform spanning tree calculation. Parameters such as the device priority and port priority affect spanning tree calculation, and the change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, configure parameters such as the device priority and port priority before enabling spanning tree protocols.

Enabling Spanning Tree Mode in MSTP

```
admin@XorPlus# set protocols spanning-tree force-version 3
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Basic Global Parameters of MSTP

When configuring global parameters, make sure to set the forward delay to greater than Max-Age/2 + 1, or the commit will fail.

```
admin@XorPlus# set protocols spanning-tree mstp bridge-priority 4096
admin@XorPlus# set protocols spanning-tree mstp forward-delay 20
admin@XorPlus# set protocols spanning-tree mstp hello-time 2
admin@XorPlus# set protocols spanning-tree mstp max-age 20
admin@XorPlus# set protocols spanning-tree mstp max-hops 8
admin@XorPlus# set protocols spanning-tree mstp configuration-name test1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# run show spanning-tree mstp bridge
Bridge Spanning Tree Parameters
Enabled Protocol: MSTP
Root ID: 4096.08:9e:01:39:1a:fe
External Root Path Cost: 0
CIST Regional Root ID: 4096.08:9e:01:39:1a:fe
Root Port:
CIST Internal Root Path Cost: 0
Hello Time: 2
Maximum Age: 20
Forward Delay: 20
Remaining Hops: 8
Bridge Configuration Name: test1
Bridge Configuration Digest: ac36177f50283cd4b83821d8ab26de62
Number of Topology Changes: 13
Time Since Last Topology Change: 0 days 00:00:31
Local Parameters
Bridge ID: 4096.08:9e:01:39:1a:fe
Hello Time: 2
Maximum Age: 20
Forward Delay: 20
Remaining Hops: 8
admin@XorPlus#
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# commit
```

```
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1
admin@XorPlus# set protocols spanning-tree mstp msti 2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 300
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 400
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree mstp bridge
Bridge Spanning Tree Parameters
Enabled Protocol: MSTP
Root ID: 4096.08:9e:01:39:1a:fe
External Root Path Cost: 0
CIST Regional Root ID: 4096.08:9e:01:39:1a:fe
Root Port:
CIST Internal Root Path Cost: 0
Hello Time: 2
Maximum Age: 20
Forward Delay: 20
Remaining Hops: 8
Bridge Configuration Name: test1
Bridge Configuration Digest: 8b5d98ca042bad0d7fa5f18744f4755d
Msti 1 Member VLANs:
100, 200,
Msti 2 Member VLANs:
300, 400,
Number of Topology Changes: 14
Time Since Last Topology Change: 0 days 00:02:49
Local Parameters
Bridge ID: 4096.08:9e:01:39:1a:fe
Hello Time: 2
Maximum Age: 20
Forward Delay: 20
Remaining Hops: 8
admin@XorPlus#
```

Configuring MSTP Interface Parameters

```
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 external-path-cost 30000
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 internal-path-cost 10000
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 edge true
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 mode point-to-point
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 port-priority 100
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# run show spanning-tree mstp interface
Spanning Tree Interface Parameters for Instance 0
Interface Port ID Designated Designated Bridge Ext Port Int Port State Role
Port ID ID Cost Cost
---------- --------- ---------- ---------------------- --------- --------- ---------- ------
ge-1/1/1 96.1 96.1 8192.08:9e:01:39:1a:fe 30000 10000 FORWARDING EDGE
```

Configuring the BPDU Filter

The BPDU filter prevents the bridge from using BPDUs for STP calculations. The switch then ignores any BPDUs that it receives.

```
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-filter true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring BPDU Root Guard

If a switch port receives a higher bridge-priority BPDU, it will ignore the BPDU and keep the current root-bridge as the root-bridge.

```
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 root-guard true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring BPDU TCN-Guard

When a port is configured with TCN-guard, the port does not process or propagate any topology change information received on the configured port.

```
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 tcn-guard true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring MSTP BPDU-Guard

When a port is configured with mstp bpdu-guard, the port which should not receive bpdu receives bpdu messages, it will be set to err-discard True and down.

```
admin@XorPlus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-guard true
admin@XorPlus# co
Commit OK.
Save done.
```

If the port is down by mstp bpdu-guard, the port status as follows.

```
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard True, Physical link is Down
Interface index: 1, Mac Learning Enabled
Port mode: access
Description: User Port
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Storm control ratio Broadcast: 1%
Interface rate limit ingress:0, egress:0
Current address: c4:39:3a:ff:2d:c1, Hardware address: c4:39:3a:ff:2d:c1
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.............................132
Output Packets............................4733
Input Octets..............................11266
Output Octets............................1664371
```

When the port is down by mstp bpdu-guard, the port will be up after you delete bpdu-guard and disable, enable the port.

```
admin@XorPlus# delete protocols spanning-tree mstp interface ge-1/1/1 bpdu-guard
admin@XorPlus# commit
Commit OK.
Save done.
```

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable true
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard False, Physical link is Up
Interface index: 1, Mac Learning Enabled
Description: User Port
Link-level type: Ethernet, MTU: 1514, Speed: 1Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Storm control ratio Broadcast: 1%
Interface rate limit  ingress:0, egress:0
Current address: c4:39:3a:ff:2d:c1, Hardware address: c4:39:3a:ff:2d:c1
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 688 bits/sec, 0 packets/sec
  Input Packets.............................132
  Output Packets............................4736
  Input Octets..............................11266
  Output Octets............................1664755
```

Disabling/Enabling MSTP

If you disable MSTP, the port will stay in forwarding status and cease to send BPDUs.

```
admin@XorPlus# set protocols spanning-tree enable false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree mstp interface
Spanning Tree Interface Parameters for Instance 0
Interface Port ID Designated Designated Bridge Ext Port Int Port State Role
Port ID ID Cost Cost
--------- ------- ---------- ---------------------- -------- -------- ---------- -------------
ge-1/1/1 96.1 96.1 8192.08:9e:01:39:1a:fe 30000 10000 FORWARDING MSTP DISABLED
ge-1/1/2 128.2 128.2 8192.08:9e:01:39:1a:fe 20000 20000 FORWARDING MSTP DISABLED
ge-1/1/13 128.13 128.13 8192.08:9e:01:39:1a:fe 20000 20000 FORWARDING MSTP DISABLED
admin@XorPlus# set protocols spanning-tree enable true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree mstp interface
Spanning Tree Interface Parameters for Instance 0
Interface Port ID Designated Designated Bridge Ext Port Int Port State Role
Port ID ID Cost Cost
--------- ------- ---------- ---------------------- -------- -------- ---------- -----------
ge-1/1/1 96.1 96.1 8192.08:9e:01:39:1a:fe 30000 10000 FORWARDING EDGE
ge-1/1/2 128.2 128.2 8192.08:9e:01:39:1a:fe 20000 20000 FORWARDING EDGE
ge-1/1/13 128.13 128.13 8192.08:9e:01:39:1a:fe 20000 20000 FORWARDING DESIGNATED
```

Configuring Root Guard

Configure Root Guard to protect devices or links. If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

```
admin@XorPlus# set protocols spanning-tree mstp interface te-1/1/3 root-guard true
admin@XorPlus# commit
```

MSTP Configuration Example

There are two examples of MSTP configuration. In our first example, VLAN 100 is mapped to MSTI-1 and VLAN 200 is mapped to MSTI-2. The entire topology belongs to only one MSTP domain named **region1**. Switch A is the root of the network.

To achieve load balancing, VLAN 100 should be in MSTI-1 (Fig. 4-4), and VLAN 200 should be in MSTI-2 (Fig. 4-5).

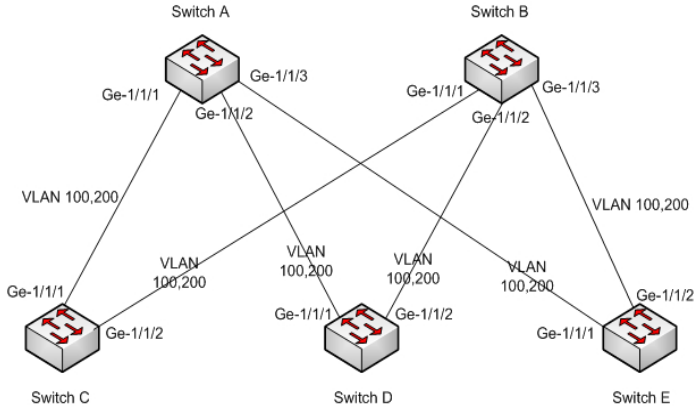


Figure 4-3. MSTP configuration.

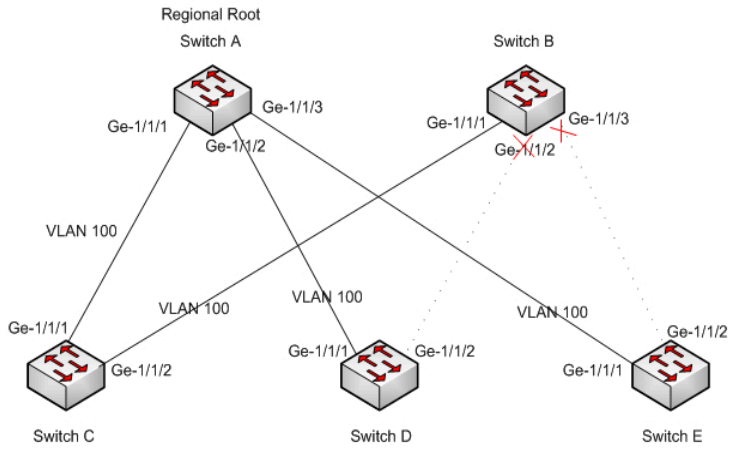


Figure 4-4. MSTI-1 topology for VLAN 100.

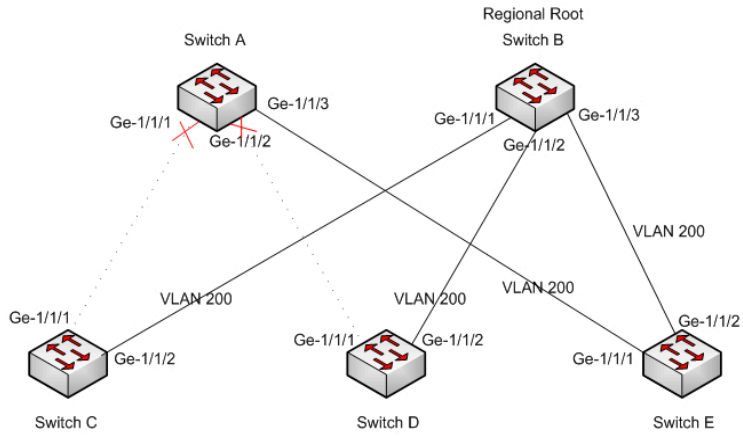


Figure 4-5. MSTI-2 topology for VLAN 200.

Configuring Switch A, Example 1

For Switch A, configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100 and VLAN 200.

```
admin@XorPlus# set vlans vlan-id 100
```

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
To make sure that Switch A is the root of the network and the regional root of MSTI-1, configure it as the higher p
admin@XorPlus# set protocols spanning-tree mstp bridge-priority 0
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch B, Example 1

Configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100 and VLAN 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch B is the regional root of MSTI-2 and that ge-1/1/2 and ge-1/1/3 are in blocking status in MSTI-1, configure a higher MSTI-2 priority and a large value for internal-path-cost in MSTI-1.

```
admin@XorPlus# set protocols spanning-tree mstp msti 2 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/2 cost 10000000
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/3 cost 10000000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch C, Example 1

Configure ge-1/1/1~ge-1/1/2 as trunk ports and as members of VLAN 100 and VLAN 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To set ge-1/1/1 and ge-1/1/2 in forwarding status in MSTI-1, configure a lower value for internal-path-cost.
To set ge-1/1/1 in blocking status in MSTI-2, configure a higher value for internal-path-cost.

```
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/1 cost 1000
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/2 cost 1000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 2 interface ge-1/1/1 cost 100000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch D, Example 1

Configure ge-1/1/1~ge-1/1/2 as trunk ports and as members of VLAN 100 and VLAN 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
```

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To set ge-1/1/1 in blocking status in MSTI-2 and ge-1/1/2 in blocking status in MSTI-1, configure a large value for internal-path-cost.

```
admin@XorPlus# set protocols spanning-tree mstp msti 2 interface ge-1/1/1 cost 10000000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/2 cost 10000000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch E, Example 1

Configure ge-1/1/1~ge-1/1/2 as trunk ports and as members of VLAN 100 and VLAN 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To set ge-1/1/1 and ge-1/1/2 in forwarding status in MSTI-2, configure a lower value for internal-path-cost.
To set ge-1/1/2 in blocking status in MSTI-1, configure a large value for internal-path-cost.

```
admin@XorPlus# set protocols spanning-tree mstp msti 2 interface ge-1/1/1 cost 1000
admin@XorPlus# set protocols spanning-tree mstp msti 2 interface ge-1/1/2 cost 1000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/2 cost 10000000
admin@XorPlus# commit
```

```
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

In the second example, there are two regions. In region 1, VLAN 100 is mapped to MSTI-1, VLAN 200 is mapped to MSTI-2, and VLAN 300 is mapped to MSTI-3. In region 2, VLAN 200 is mapped to MSTI-2 and VLAN 400 is mapped to MSTI-4. Switch A is the root of the entire network. The topologies of the VLANs are presented in Fig. 4-6 through 4-10.

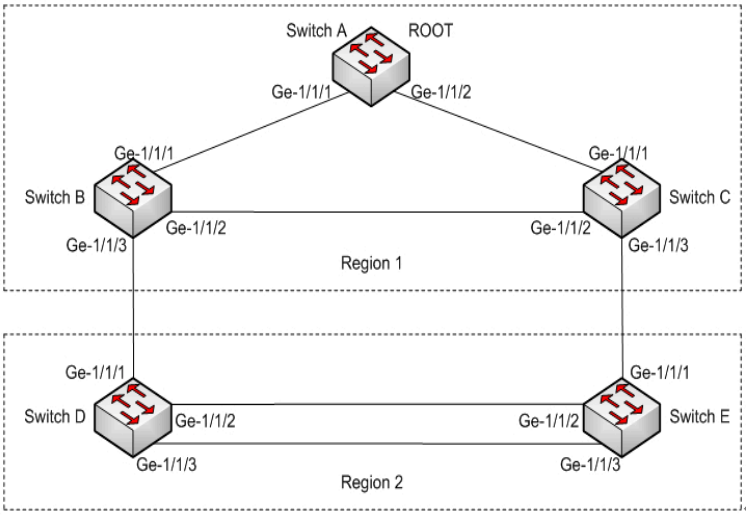


Figure 4-6. MSTP configuration.

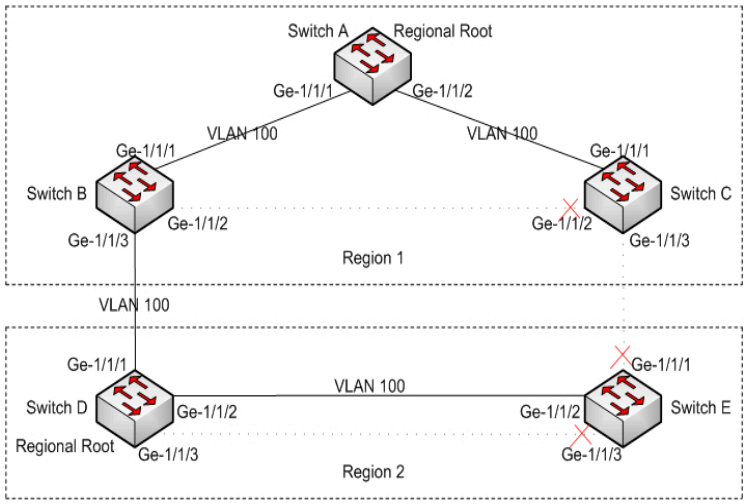


Figure 4-7. Topology for VLAN 100.

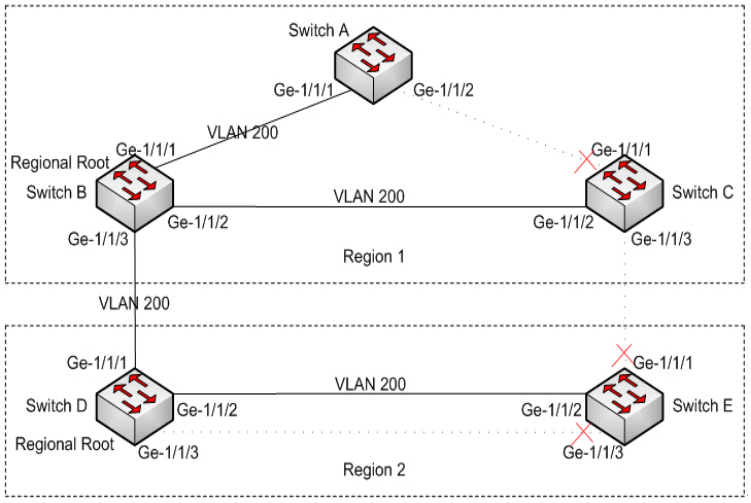


Figure 4-8. Topology for VLAN 200.

Figure 4-9. Topology for VLAN 300.

Figure 4-10. Topology for VLAN 400.

Configuring Switch A, Example 2

For Switch A, configure ge-1/1/1~ge-1/1/2 as trunk ports and as members of VLAN 100, VLAN 200, VLAN 300, and VLAN 400.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 400
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 3 vlan 300
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
```

```
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
To verify that Switch A is the root of the network and the regional root of MSTI-1, configure it as the higher pri
admin@XorPlus# set protocols spanning-tree mstp bridge-priority 0
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 1 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch B, Example 2

Configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100, VLAN 200, VLAN 300, and VLAN 400.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 400
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 3 vlan 300
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch B is the regional root of MSTI-2 and that ge-1/1/1 is in blocking status in MSTI-3, configure a higher MSTI-2 priority and a large value for internal-path-cost in MSTI-3.

```
admin@XorPlus# set protocols mstp msti 2 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols mstp msti 3 interface ge-1/1/1 cost 10000000
admin@XorPlus# commit
Waiting for merging configuration.
```

```
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch C, Example 2

Configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100, VLAN 200, VLAN 300, and VLAN 400.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 400
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 1 vlan 100
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 3 vlan 300
admin@XorPlus# set protocols spanning-tree mstp configuration-name region1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch C is the regional root of MSTI-3, ge-1/1/1 is in blocking status in MSTI-2, and ge-1/1/2 is in blocking status in MSTI-1, user should configure a higher MSTI-3 priority and large values for internal-path-costs of ge-1/1/1 in MSTI-2 and ge-1/1/2 in MSTI-1.

```
admin@XorPlus# set protocols spanning-tree mstp msti 3 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 2 interface ge-1/1/1 cost 10000000
admin@XorPlus# set protocols spanning-tree mstp msti 1 interface ge-1/1/2 cost 10000000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch D, Example 2

Configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100, VLAN 200, VLAN 300, and VLAN 400.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
```

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 400
admin@XorPlus#
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 4 vlan 400
admin@XorPlus# set protocols spanning-tree mstp configuration-name region2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch D is the regional root of MSTI-2 and the root of CIST. Configure a higher MSTI-2 priority and bridge priority.

```
admin@XorPlus# set protocols spanning-tree mstp bridge-priority 16384
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree mstp msti 2 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch E, Example 2

Configure ge-1/1/1~ge-1/1/3 as trunk ports and as members of VLAN 100, VLAN 200, VLAN 300, and VLAN 400.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 400
admin@XorPlus#
admin@XorPlus# commit
```

```
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree mstp msti 2 vlan 200
admin@XorPlus# set protocols spanning-tree mstp msti 4 vlan 400
admin@XorPlus# set protocols spanning-tree mstp configuration-name region2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch E is the regional root of MSTI-4. Configure a higher MSTI-4 priority.

```
admin@XorPlus# set protocols spanning-tree mstp msti 4 bridge-priority 4096
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Rapid PVST+ Configuration

802.1D, 802.1w, and 802.1s are spanning tree protocols that avoid the loop in Layer 2. You can configure the parameters of rapid-PVST+, including bridge-priority, forward-delay, max-age, and hello-time interval.

NOTE:

- On a chassis switch, a maximum of 64 VLANs can be enabled for rapid-PVST+ mode.
- Once the spanning tree protocol is enabled on the network, the port starts to perform spanning tree calculation. Parameters such as the device priority and port priority affect spanning tree calculation, and the change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, configure parameters such as the device priority and port priority before enabling spanning tree protocols.
- For rapid-PVST+ in PICOS switches, the value of **Organization Code** field in the BPDUs is 00:00:00. The peer devices with a different value should ignore the compatibility check of this field, otherwise, it may cause device connection problems due to compatibility issues.
- Rapid PVST+ blocks traffic from the dynamic VLAN delivered from the RADIUS authentication server.

When using rapid-PVST+, pay attention to the following two points:

- For the trunk port
  - In VLAN 1 and the native VLAN, the rapid-PVST+ device sends standard RSTP and rapid-PVST+ packets (untagged, the destination MAC address is 01-80-C2-00-00-00) to negotiate with the peer.
  - In other VLANs, the rapid-PVST+ device sends rapid-PVST+ packets (the destination MAC address is 01-00-0C-CC-CC-CD) to negotiate with the peer.
- For the access port
  - In all VLANs, the rapid-PVST+ device sends only standard RSTP packets to negotiate with the peer.

Enabling Spanning Tree Mode in Rapid PVST+

```
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Basic VLAN Parameters of Rapid PVST+

When configuring basic VLAN parameters, set the forward delay to greater than Max-Age/2 + 1, or the commit will fail.

```
admin@XorPlus# set protocols spanning-tree pvst vlan 2 bridge-priority 4096
admin@XorPlus# set protocols spanning-tree pvst vlan 2 forward-delay 20
admin@XorPlus# set protocols spanning-tree pvst vlan 2 hello-time 4
admin@XorPlus# set protocols spanning-tree pvst vlan 2 max-age 30
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree pvst bridge vlan 2
PVST Bridge Parameters for VLAN 2
Root Bridge: 4098.08:9e:01:61:65:71
Root Cost: 0
Root Port:
Hello Time: 4
Max Age: 30
Forward Delay: 20
Time Since Last Topology Change: 0 days 00:02:55
Local Parameters
Bridge ID: 4098.08:9e:01:61:65:71
Hello Time: 4
Maximum Age: 30
Forward Delay: 20
```

Configuring Rapid PVST+ Interface Parameters

```
admin@XorPlus# set protocols spanning-tree pvst vlan 2 interface ge-1/1/1 path-cost 555555
```

```
admin@XorPlus# set protocols spanning-tree pvst vlan 2 interface ge-1/1/1 port-priority 200
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# run show spanning-tree pvst interface vlan 2
Rapid PVST+ Spanning Tree Interface Status for VLAN 2
Interface Port ID Designated Designated Bridge Port Cost State Role
Port ID ID
---------- --------- ---------- ---------------------- --------- ---------- ---------------
ge-1/1/1 192.1 192.1 4098.08:9e:01:61:65:71 555555 FORWARDING EDGE
```

Configuring the Interface Mode

You can configure the interface mode as point-to-point or shared.

```
admin@XorPlus# set protocols spanning-tree pvst interface ge-1/1/1 mode point-to-point
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree pvst interface ge-1/1/1 mode shared
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Rapid PVST+ BPDU-guard

When a port is configured with pvst bpdu-guard, the port which should not receive bpdu receives bpdu messages, it will be set to err-discard True and down.

```
admin@XorPlus# set protocols spanning-tree pvst interface ge-1/1/1 bpdu-guard true
admin@XorPlus# co
Commit OK.
Save done.
```

If the port is down by pvst bpdu-guard, the port status as follows.

```
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard True, Physical link is Down
Interface index: 1, Mac Learning Enabled
Port mode: access
Description: User Port
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Storm control ratio Broadcast: 1%
Interface rate limit ingress:0, egress:0
Current address: c4:39:3a:ff:2d:c1, Hardware address: c4:39:3a:ff:2d:c1
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.............................132
Output Packets............................4733
Input Octets..............................11266
Output Octets............................1664371
```

When the port is down by pvst bpdu-guard, the port will be up after you delete bpdu-guard and disable, enable the port.

```
admin@XorPlus# delete protocols spanning-tree pvst interface ge-1/1/1 bpdu-guard
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable true
admin@XorPlus# commit
Commit OK.
```

```
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 disable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard False, Physical link is Up
Interface index: 1, Mac Learning Enabled
Port mode: access
Description: User Port
Link-level type: Ethernet, MTU: 1514, Speed: 1Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Storm control ratio Broadcast: 1%
Interface rate limit  ingress:0, egress:0
Current address: c4:39:3a:ff:2d:c1, Hardware address: c4:39:3a:ff:2d:c1
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 688 bits/sec, 0 packets/sec
  Input Packets.............................132
  Output Packets............................4736
  Input Octets..............................11266
  Output Octets............................1664755
```

Disabling/Enabling Rapid PVST+ on One VLAN

You can disable or enable the spanning tree protocol PVST on a single designated VLAN.

```
admin@XorPlus# set protocols spanning-tree pvst vlan 2 enable false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree pvst bridge vlan 2
PVST Bridge Parameters for VLAN 2
Root Bridge: 32769.08:9e:01:61:65:71
Root Cost: 0
Root Port:
Hello Time: 2
Max Age: 20
Forward Delay: 15
Time Since Last Topology Change: 15804 days 23:00:11
Local Parameters
Bridge ID: 32769.08:9e:01:61:65:71
Hello Time: 2
Maximum Age: 20
Forward Delay: 15
admin@XorPlus# set protocols spanning-tree pvst vlan 2 enable true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree pvst bridge vlan 2
PVST Bridge Parameters for VLAN 2
Root Bridge: 4098.08:9e:01:61:65:71
Root Cost: 0
Root Port:
Hello Time: 4
Max Age: 30
Forward Delay: 20
Time Since Last Topology Change: 0 days 00:00:21
Local Parameters
Bridge ID: 4098.08:9e:01:61:65:71
Hello Time: 4
Maximum Age: 30
Forward Delay: 20
```

```
admin@XorPlus#
```

Disabling/Enabling Rapid PVST+

You cannot disable the spanning tree protocol rapid-PVST+ with just the **enable false** command. To disable PVST, *first* configure the spanning tree mode in MSTP/RSTP/STP. Then, disable the spanning tree. After the spanning tree is disabled, the port will stay in "forwarding" status and cease to send BPDUs.

```
admin@XorPlus# set protocols spanning-tree enable false
admin@XorPlus# commit
Waiting for merging configuration.
Commit Failed
102 Command failed Cannot disable spanning tree under PVST mode[
admin@XorPlus#
admin@XorPlus# exit discard
admin@XorPlus> configure
Entering configuration mode.
There are no other users in configuration mode.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree enable false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols spanning-tree enable true
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run show spanning-tree
Bridge Spanning Tree Parameters
Enabled Protocol: PVST
Root ID: 32769.08:9e:01:61:65:71
Root Path Cost: 0
Designated Bridge ID: 32769.08:9e:01:61:65:71
Root Port:
Hello Time: 2
Maximum Age: 20
Forward Delay: 15
Number of Topology Changes: 1
Time Since Last Topology Change: 0 days 00:00:09
Local Parameters
Bridge ID: 32769.08:9e:01:61:65:71
Hello Time: 2
Maximum Age: 20
Forward Delay: 15
```

Configuring Root Guard

Configure Root Guard to protect devices or links. If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

```
admin@XorPlus# set protocols spanning-tree pvst interface te-1/1/3 root-guard true
admin@XorPlus# commit
```

Rapid PVST+ Configuration Example

The following topology is an example of a rapid-PVST+ configuration. Switches A and B are in the aggregation layer, and switches C and D are in the access layer. Configure switch A as the root bridge of VLAN 100 and VLAN 200, switch B as the root bridge of VLAN 300, and switch C as the root bridge of VLAN 400.

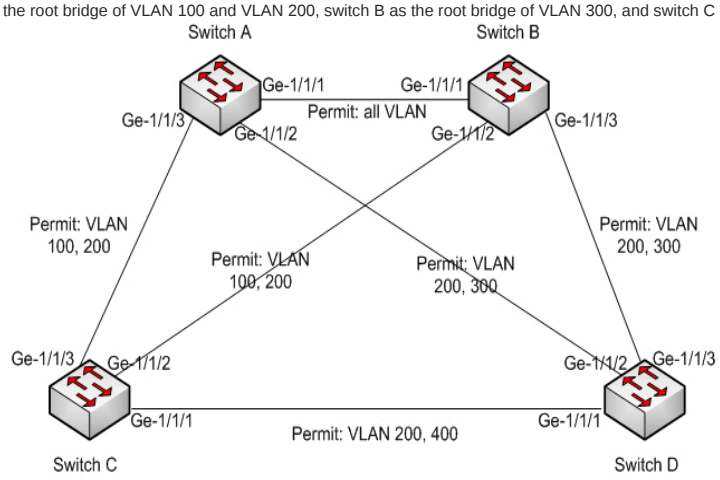


Figure 4-11. PVST configuration.

Configuring Switch A

For Switch A, configure ge-1/1/1~ge-1/1/3 as trunk ports; ge-1/1/1 as a member of VLANs 100, 200, 300, and 400; ge-1/1/2 as a member of VLANs 200 and 300; and ge-1/1/3 as a member of VLANs 100 and 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch A is the root bridge of VLANs 100 and 200, configure VLANs 100 and 200 as the higher priority.

```
admin@XorPlus# set protocols spanning-tree pvst vlan 100 bridge-priority 0
admin@XorPlus# set protocols spanning-tree pvst vlan 200 bridge-priority 0
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch B

Configure ge-1/1/1~ge-1/1/3 as trunk ports, and ge-1/1/1 as a member of VLANs 100, 200, 300, and 400; ge-1/1/2 as a member of VLANs 100 and 200; and ge-1/1/3 as a member of VLANs 200 and 300.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch B is the root bridge of VLAN 300, configure VLAN 300 as the higher priority.

```
admin@XorPlus# set protocols spanning-tree pvst vlan 300 bridge-priority 0
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch C

Configure ge-1/1/1~ge-1/1/3 as trunk ports; ge-1/1/1 as a member of VLANs 200 and 400; ge-1/1/2 as a member of VLANs 100 and 200; and ge-1/1/3 as a member of VLANs 100 and 200.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

To verify that Switch C is the root bridge of VLAN 400, configure VLAN 400 as the higher priority.

```
admin@XorPlus# set protocols spanning-tree pvst vlan 400 bridge-priority 0
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Switch D

Configure ge-1/1/1~ge-1/1/3 as trunk ports; ge-1/1/1 as a member of VLANs 200 and 400; ge-1/1/2 as a member of VLANs 200 and 300; and ge-1/1/3 as a member of VLANs 200 and 300.

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set vlans vlan-id 300
admin@XorPlus# set vlans vlan-id 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 300
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set protocols spanning-tree force-version 4
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

BPDU Tunneling Configuration

Introduction

As a Layer 2 tunneling technology, BPDU tunneling enables Layer 2 protocol packets from geographically dispersed customer networks to be transparently transmitted over a BPDU tunnel on the ISP (Internet Service Provider) network.

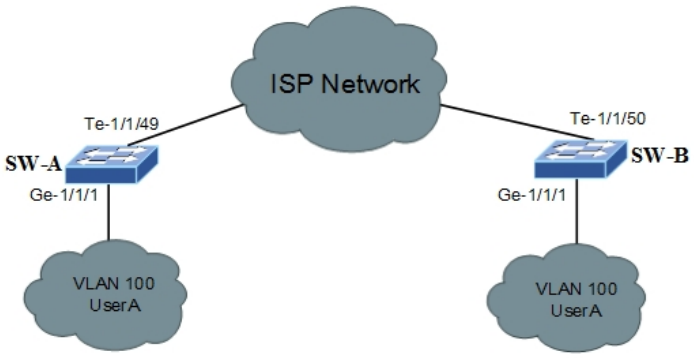


Figure 1 Transparent Transmission of Layer 2 Protocol Packets through BPDU Tunnel

PicOS currently supports Layer 2 protocol packets of STP and LACP that can be transmitted through BPDU tunneling. Transparent transmission of Layer 2 protocol packets through BPDU tunnel is based on the following processes:

1. On the BPDU tunnel ingress switch SW-A, destination multicast MAC address of the received Layer 2 protocol packet is replaced with a specified destination multicast MAC address.

2. Layer 2 protocol packets are transparently transmitted through the ISP network.

3. When the packet arrives at the BPDU tunnel egress switch SW-B, the destination multicast MAC address is checked and the packet is considered as a tunneled packet. Then the destination multicast MAC address of the packet is restored to standard destination multicast MAC address on the BPDU tunnel egress interface, and the packet is further processed and forwarded.

Configuration Notes

- BPDU Tunneling cannot be configured on a LAG port or a physical port that belongs to a LAG. When we need to configure BPDU tunneling on the physical port that belongs to a LAG, we must first remove the physical port from the LAG port before configuration.
- When configuring BPDU tunneling destination multicast MAC address, the following multicast MAC addresses cannot be used:

  01:80:C2:00:00:00 to 01:80:C2:00:00:2f.
- The destination multicast MAC address configured on the tunnel ingress switch and the egress switch must be the same value.

Configuring BPDU Tunneling

Procedure

Step1 Configure VLAN.

a) Configure VLAN ID.

set vlans <*vlan-id*>

b) Configure the interface to VLAN.

set interface gigabit-ethernet <*port-id*> **family ethernet-switching vlan members** <*vlan-id*>

Step2 Enable the BPDU tunneling function of the Layer 2 protocol.

set interface gigabit-ethernet <*port-id*> **family ethernet-switching bpdu-tunneling protocol** <*protocol-type*>

Step3 Configure the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

set interface bpdu-tunneling destination-mac <*destination-mac*>

Configuration Example

Network Requirements

1. Private networks of User A and User B are located on two sides of the ISP network, as shown in Figure 2, SwitchA1, SwitchA2, SwitchB1 and SwitchB2 are the edge devices of the user network, SW-A and SW-B are the edge devices of the ISP network.
2. The User A network belongs to VLAN 100 and the User B network belongs to VLAN 200.

3. The BPDU tunneling function of the STP protocol is enabled so that Layer 2 protocol packets of User A and User B can cross the ISP network to complete the spanning tree calculation.

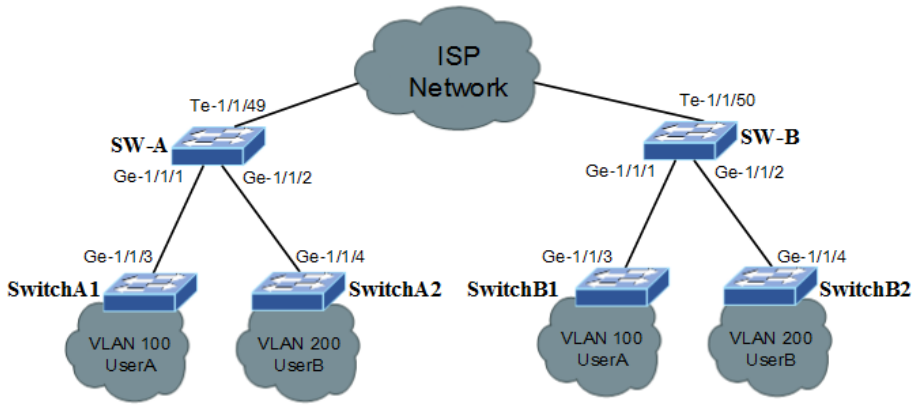


Figure 2 Networking Diagram for Configuring Transparent Transmission of Layer 2 Protocol Packets through BPDU Tunnel

Procedure

Step1 Enable STP function on SwitchA1, SwitchA2, SwitchB1 and SwitchB2.

 # Configure SwitchA1

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@XorPlus# set protocols spanning-tree enable true
```

 # Configure SwitchA2

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching vlan members 200
admin@XorPlus# set protocols spanning-tree enable true
```

 # Configure SwitchB1

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan  members 100
admin@XorPlus# set protocols spanning-tree enable true
```

 # Configure SwitchB2

```
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching vlan members 200
admin@XorPlus# set protocols spanning-tree enable true
```

Step2 Configure VLAN on SW-A and SW-B.

 # Configure SW-A

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 family ethernet-switching vlan members 200
```

 # Configure SW-B

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set vlans vlan-id 200
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
```

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 200
admin@XorPlus# set interface gigabit-ethernet te-1/1/50 family ethernet-switching port- mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/50 family ethernet-switching vlan members 100
admin@XorPlus# set interface gigabit-ethernet te-1/1/50 family ethernet-switching vlan members 200
```

Step3 Enable the BPDU tunneling function of STP on SW-A and SW-B of different inbound interface.

 # Configure SW-A

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching bpdu-tunneling protocol stp
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family Ethernet-switching bpdu-tunneling protocol stp
```

 # Configure SW-B

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching bpdu-tunneling protocol stp
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching bpdu-tunneling protocol stp
```

Step4 Configure the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

 # Configure SW-A

```
admin@XorPlus# set interface bpdu-tunneling destination-mac 01:90:00:00:00:1a
```

 # Configure SW-B

```
admin@XorPlus# set interface bpdu-tunneling destination-mac 01:90:00:00:00:1a
```

> **NOTE:**
>
> The destination multicast MAC address configured on the tunnel ingress switch and the egress switch must be the same value.

Configuring Flex Links Preemption Delay

User can configure two physical ports or two LAGs as Flex Links or configure one physical port and one LAG as Flex Links.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 backup-port interface ae1
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 backup-port delay 10
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set interface aggregate-ethernet ae2 backup-port interface ae3
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Configuring the Preemption Mode

By default, the preemption mode is set, and the active interface is preferred. Beyond that, user can configure the "bandwidth" or "off" mode. The "bandwidth" mode calls for a higher bandwidth interface, and the "off" mode turns off preemption.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 backup-port mode bandwidth
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Showing Flex Links on All Interfaces

User can view the state of user's Flex Links interfaces:

```
admin@XorPlus# run show interface flexlink
Active Interface Backup Interface Mode Delay(seconds)
---------------- ---------------- --------- --------------
ge-1/1/1(up) ge-1/1/2(standby) bandwidth 10
admin@XorPlus#
```

UDLD Configuration

UDLD (Unidirectional Link Detection) using for detecting optical fiber unidirectional link. It supports two modes of operation: normal mode(the default) and aggressive mode. In normal mode, UDLD can detect unidirectional links due to mis-connected interfaces. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic, twisted-pair links, and mis-connected interfaces. You can enable UDLD globally or on specific ports. When UDLD detectes uni-directional fault, the port status will be setted Disabled(UDLD) and down, and there is no udld neighbor. In addition, UDLD can detect the self loop port and disable this port. Self loop means TX links to RX on the same port.

Caution:

- For the case of TX-RX (RX indicates the receiving end, and TX indicates the sending end) self-loops on one ethernet port, the port status will be set to Disabled (UDLD) and down, and there will be no UDLD neighbor.
- Do not configure up-mode with UDLD, as this may cause the peer interface to be disabled unexpectedly by UDLD.

Configure UDLD normal mode on global

```
admin@XorPlus# set protocols udld disable false
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure UDLD aggressive mode on global

```
admin@XorPlus# set protocols udld disable false
admin@XorPlus# set protocols udld aggressive true
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure UDLD normal mode on Specific Port

```
admin@XorPlus# set protocols udld interface te-1/1/27 disable false
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure UDLD aggressive mode on Specific Port

```
admin@XorPlus# set protocols udld interface te-1/1/27 disable false
admin@XorPlus# set protocols udld interface te-1/1/27 aggressive true
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
```

Configure UDLD Message-interval

```
admin@XorPlus# set protocols udld message-interval 20
admin@XorPlus# commit
Commit OK.
Save done.
```

UDLD status as follows when the link is good

```
admin@Xorplus# run show udld neighbors
  Port       Device Name     Device ID        Port ID     state
--------     -----------    -----------    ------------   ---------------
```

```
te-1/1/27    3295           QTFQXI10700003  te-1/1/49      bi-directional

admin@Xorplus# run show udld interface te-1/1/27
Interface te-1/1/27
---------------------------------------
Udld enabled, aggressive mode
Current bidirectional state: bi-directional
Current phase: advertisement
Message interval: 15s
Timeout interval: 5s
    neighbor 1
    -----------------
    Expiration time: 43.58s
    Device ID: QTFQXI10700003
    Port ID: te-1/1/49
    Message interval: 20s
    Timeout interval: 5s
    Device name: 3295
```

UDLD status as follows when UDLD detect uni-directional fault

```
admin@Xorplus# run show udld neighbors
  Port       Device Name     Device ID        Port ID     state
--------     -----------    -----------    ------------   ---------------

admin@Xorplus# run show udld interface te-1/1/27
Interface te-1/1/27
---------------------------------------
Udld enabled
Current bidirectional state: uni-directional
Current phase: linkdown
Message interval: 7s
Timeout interval: 5s

admin@XorPlus# run show interface gigabit-ethernet te-1/1/27
Physical interface: te-1/1/27, Enabled, error-discard True(UDLD), Physical link is Down
Interface index: 27, SFP type: SR/850
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Current address: 00:90:4c:06:a5:73, Hardware address: 00:90:4c:06:a5:73
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.............................16
  Output Packets............................1360
  Input Octets..............................1797
  Output Octets............................157178
```

UDLD status when self loop link

The example is that tx connect with rx on the same port te-1/1/27. The udld status will be transmit-to-receive loop, and the port status will be setted Disabled(UDLD) and down, and there is no udld neighbor.

```
admin@Xorplus# run show udld neighbors
  Port       Device Name     Device ID        Port ID     state
--------     -----------    -----------    ------------   ---------------

admin@Xorplus# run show udld interface te-1/1/27
Interface te-1/1/27
---------------------------------------
Udld enabled, aggressive mode
Current bidirectional state: transmit-to-receive loop
Current phase: linkdown
Message interval: 7s
```

```
Timeout interval: 5s

admin@XorPlus# run show interface gigabit-ethernet te-1/1/27
Physical interface: te-1/1/27, Disabled(UDLD), error-discard False, Physical link is Down
Interface index: 27, SFP type: SR/850
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Precision Time Protocol mode:none
Current address: 00:90:4c:06:a5:73, Hardware address: 00:90:4c:06:a5:73
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.............................16
  Output Packets............................1360
  Input Octets..............................1797
  Output Octets............................157178
```

Recover port status Disabled(UDLD)

You can through down, up the port to recover the status Disabled(UDLD)

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/27 disable true
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface gigabit-ethernet te-1/1/27 disable false
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show interface gigabit-ethernet te-1/1/27
Physical interface: te-1/1/27, Enabled, error-discard False, Physical link is Up
Interface index: 27, SFP type: SR/850
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Precision Time Protocol mode:none
Current address: 00:90:4c:06:a5:73, Hardware address: 00:90:4c:06:a5:73
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.............................16
  Output Packets............................1360
  Input Octets..............................1797
  Output Octets............................157178
```

Or you can using follow command to recover the status Disabled(UDLD)

```
admin@XorPlus# run clear udld
admin@XorPlus# run show interface gigabit-ethernet te-1/1/27
Physical interface: te-1/1/27, Enabled, error-discard False, Physical link is Up
Interface index: 27, SFP type: SR/850
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Precision Time Protocol mode:none
Current address: 00:90:4c:06:a5:73, Hardware address: 00:90:4c:06:a5:73
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
```

```
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.....................16
Output Packets....................1360
Input Octets......................1797
Output Octets.....................157178
```

LFS Configuration

Abstract

Link fault signaling (LFS) operates between the remote RS and the local RS. Faults detected between the remote RS and the local RS are received by the local RS as Local Fault. RS is the only layer that can generate Remote Fault signals.

Sublayers within the PHY are capable of detecting faults that render a link unreliable for communication. Upon recognition of a fault condition, a PHY sublayer indicates Local Fault status on the data path. When this Local Fault status reaches an RS, the RS stops sending MAC data, and continuously generates a Remote Fault status on the transmit data path (possibly truncating a MAC frame being transmitted). When Remote Fault status is received by an RS, the RS stops sending MAC data, and continuously generates Idle control characters. When the RS no longer receives fault status messages, it returns to normal operation, sending MAC data.

The RS reports the fault status of the link. Local Fault indicates a fault detected on the receive data path between the remote RS and the local RS. Remote Fault indicates a fault on the transmit path between the local RS and the remote RS.

The fault status is as follows:

a) link_fault = OK

The RS shall send MAC frames as requested through the PLS service interface. In the absence of MAC frames, the RS shall generate Idle control characters.

b) link_fault = Local Fault

The RS shall continuously generate Remote Fault Sequence ordered_sets.

c) link_fault = Remote Fault

The RS shall continuously generate Idle control characters.

Link Fault Signaling

If ignore local fault is set as false: When link local fault is triggered, the RS shall continuously generate Remote Fault Sequence ordered_sets. Otherwise, the RS will not generate Remote Fault Sequence ordered_sets.

If ignore remote fault is set as false: When link remote fault is received, the RS shall continuously generate Idle control characters. Otherwise, the RS shall send MAC frames as requested through the PLS service interface and generate Idle control characters in the absence of MAC frames

LFS Commands

The following is the configuration command as sample:

```
set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-local-fault true/false
set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-remote-fault true/fals
```

Up Mode

The force up command forcibly brings up a fiber Ethernet port and enables the port to forward packets unidirectionally over a single link. In this way, transmission links are well utilized.

Up Mode Commands

The following is the configuration commad as sample:

```
set interface gigabit-ethernet te-1/1/1 up-mode true/false
```

> ⚠ Up-mode true command should be configured with ignore-local-fault true command together. If user only configures up-mode true and does not configure ignore-local-fault command, traffic cannot transmit from TX link.

Storm Control in Ethernet Port Configuration

You can configure unicast, multicast, and broadcast storm control in packets per second, kilobits per second or percentage of physical link speed. The storm control function can permit the max rate of unicast, multicast, and broadcast traffics on ingress port.

- Storm-control function is invalid for the known unicast traffic. It works on the unknown unicast, all multicast and broadcast traffic.
- pps, kbps and ratio are mutually exclusive and can not be configured at the same time.
- When the value of the storm control is set to 0, it means that data packets are not allowed to pass.
- For storm control in kbps, the actual value of storm control and the configured value are not exactly the same, the correspondence is:

  When the configured value is between 64*n and 64*n+63, where n is an integer, the actual value of the storm control is 64*n. For example, when the configured value is 200 kbps (between 64*3 and 255), the actual value of the storm control is 64*3=192 kbps. There is a special case, when the configured value is between 0 and 63, the actual value of the flow control is 64 kbps.

Configuring Storm Control in packet per second on ingress port

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast pps 10000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control multicast pps 10000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control unicast pps 10000
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Storm Control in ratio on ingress port

The ratio means the percentage of the physical link speed.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 storm-control broadcast ratio 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 storm-control multicast ratio 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 storm-control unicast ratio 30
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Storm Control in kilobits per second on ingress port

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast kbps 1000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control multicast kbps 1000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control unicast kbps 1000
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Ethernet Ring Protection Switching (ERPS)

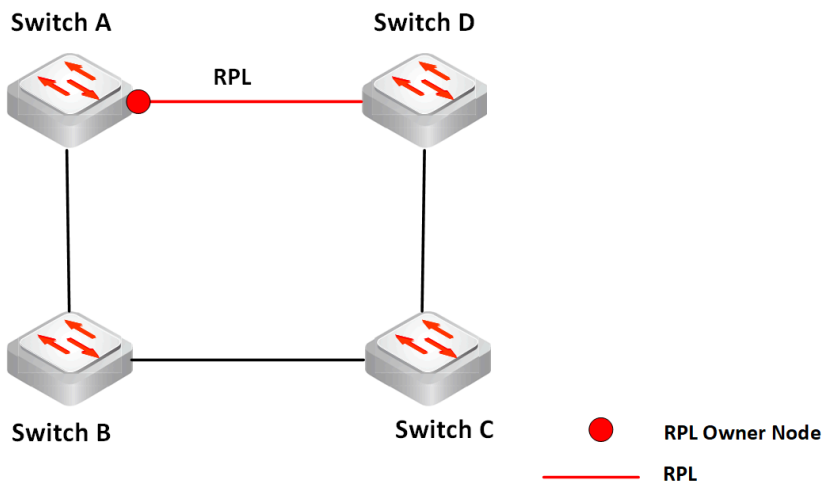
- Overview of ERPS
- Configuration Notes and Constraints of ERPS
- Configuring ERPS
- Example for Configuring ERPS (Single Ring)
- Example for Configuring ERPS (Intersection Rings)

Overview of ERPS

- Terminology
  - Ring, Major Ring and Sub-ring
  - Ring Instance
  - Node
  - Port Role
  - Control VLAN
  - Data VLAN
  - Protected Instance
  - ERPS Timer
  - Revertive/Non-revertive Mode
  - Port Blocking Switching Method
- Virtual-Channel Sub-ring RAPS Message Transmission Method
- Non-Virtual-Channel Sub-ring RAPS Message Transmission Method
- Connect Ring for Sub-ring
- Tcn-propagation
- ERPS Operation Mechanism
  - Link Failure
  - Recovery of Link Failure

Redundant links (e.g., ring networks) are often used in Ethernet switching networks for link backup and to improve network reliability. However, redundant links always form loops in the network, which may cause broadcast storms and unstable MAC address tables, and result in undesirable network communication interruption for users.

Figure 1. ERPS Diagram



As shown in **Figure 1**, Ethernet Ring Protection Switching (ERPS) is a layer 2 ring protection protocol standard defined by ITU-T under the standard number ITU-T G.8032/Y1344. It defines the Ring Auto Protection Switching (RAPS) protocol message and ring protection mechanism.

PICOS supports both versions of ERPSv1 and ERPSv2. ERPSv2 is fully compatible with ERPSv1 and has the following extensions:

- Sub-ring supporting
- Sub-ring virtual channel/non-virtual channel transmission of RAPS messages
- Manual switching of port blocking, including Forced Switch and Manual Switch
- ERPS ring revertive/non-revertive modes are configurable
- Sub-ring topology change notifications

ERPSv1 only supports major ring networking, while ERPSv2 supports not only major ring, but also supports sub-ring network, and the mixed networking of major ring and sub-ring.

ERPS leverages the advantages of ring protection technologies such as STP, with optimized detection mechanism and faster convergence; it also has good compatibility to allow interoperability with the switches, also support ERPS protocol, of other manufacturers within the ring.

Terminology

Ring, Major Ring and Sub-ring

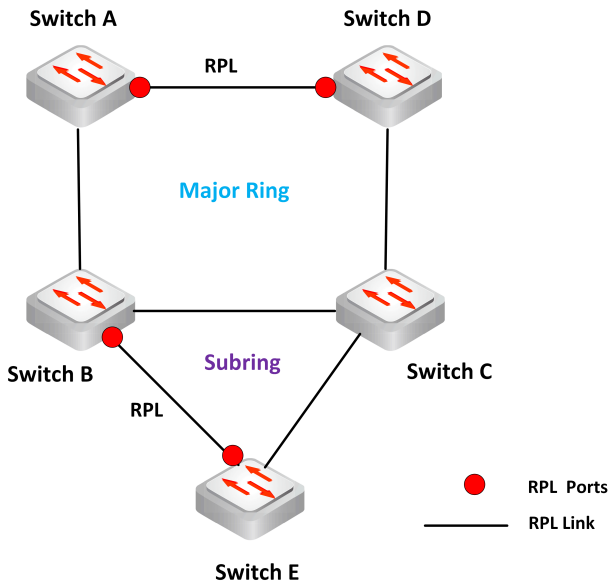
A group of interconnected Layer 2 switching devices configured with the same control VLAN and is the basic unit of the ERPS protocol forms an ERPS ring.

An ERPS ring can be a major ring or a sub-ring. By default, an ERPS ring is a major ring. The major ring is a closed ring, and the sub-ring is a non-closed ring which needs to be defined by CLI command **set protocols erps ring** *<ring-id>* **sub-ring** <**true | false**>. The configuration of the sub-ring is supported only in ERPSv2 version.

The Ethernet ring control module supports multiple rings in each node (two interfaces are part of each ring). The ring control module also supports the intersection of multiple rings. Intersection of two rings means that two rings might share the same link or share the same node.

As shown in **Figure 2**, Switch A, Switch B, Switch C and Switch D form an ERPS major ring, Switch B, Switch C and Switch E form an ERPS sub-ring. The ring ID is a unique identifier for each physical ring which can be configured by command **set protocols erps ring** *<ring-id>*.

Figure 2. ERPS Major Ring and Sub-ring



The protocol messages of the major ring are transmitted only on the major ring, and the protocol messages of the sub-ring will terminate at the intersecting nodes and will not enter the major ring. However, when there is a link fault in the sub-ring, it is necessary to advertise the topology change information of the sub-ring to the major ring at the intersecting nodes Switch B and Switch C, which is fulfilled by the tcn-propagation function.

Users can plan and deploy ERPS major ring and sub-ring by accordance with the actual network topology and usage environment.

Ring Instance

The ERPS ring is a physical ring, and the ring instance can be understood as a logical ring on the physical ring. A maximum of eight ERPS rings (including both major ring and sub-ring) are supported on a device, and a maximum of two instances can be configured for each ring. Additionally, at least one instance should be configured for each ring.

To improve link utilization, ERPS supports the configuration of up to two logical ERPS rings on a single physical ring, i.e., two instances. Usually, different instances should have unique configurations such as port roles, control VLANs, etc. Each instance has its own blocking port, which will be blocked or unblocked separately, without affecting other instances. Topology calculation for different instances will not affect each other.

For example, different protected instances can be configured for different ring instances, data traffic belonging to different VLANs can then be transmitted through different paths, thus achieving load sharing and link backup of traffic and maximizing the utilization of link resources.

Node

The Layer 2 switching devices that join the ERPS ring are called ERPS nodes. No more than two ports per node can join the same ERPS ring, which are named ERPS **port0** and **port1**.As shown in **Figure 2**, Switch A, Switch B Switch C and Switch D are the nodes of the major ring, Switch B, Switch C and Switch E are the nodes of the sub-ring.

Port Role

There are three types of ERPS port role: RPL Owner Port, RPL Neighbor Port and Ordinary Port.

- RPL Owner Port

Each ERPS ring instance has only one RPL owner port, which is determined by user configuration. By blocking the RPL owner port to forward user traffic, it prevents network loops in the ERPS ring. RPL owner port state is discarding, it can only send and receive ERPS protocol packets.

When the device of the RPL owner port receives a link failure message and learns that other nodes or links on the ERPS ring are down, it will automatically unblock the RPL owner port. RPL owner port state changes to forwarding, which will resume receiving and sending traffic, ensuring that traffic will not be interrupted.

The link where the RPL owner port located is the Ring Protection Link (RPL), which is normally NOT allowing traffic to pass.

- RPL Neighbor Port

RPL neighbor port refers to the port on the RPL link that is directly connected to the RPL owner port. It needs to be specified by the user configuration.

In normal condition, both the RPL owner port and the RPL neighbor port are blocked to prevent network loop.

When a link failure occurs, both the RPL owner port and the RPL neighbor port will be unlocked.

- Ordinary Port

The ERPS port is an ordinary port if not specified as an RPL owner port or RPL neighbor port.

The ordinary ports are responsible for monitoring the link status of the ERPS ring and informing other ring nodes.

Control VLAN

In an ERPS ring, the control VLAN is used to transmit ERPS protocol packets.

- Each ERPS ring instance must be configured with a control VLAN.
- Different ERPS ring instances cannot use the same control VLAN.

- The same control VLAN must be configured for all devices in the same ERPS ring instance.

Data VLAN

Data VLANs are a group of VLAN(s) that is used in the ring for transmission of user traffic, which should be defined in MSTP instance and VLAN mapping.

Protected Instance

Protected instance is the MSTP instance of data VLAN mapping that needs the ERPS ring protection. Before configuring ERPS, users need to configure protected MSTP instance and VLAN mapping by using command **set protocols spanning-tree mstp msti** <*msti*> **vlan** <*vlan-id*>. Then, configure the MSTP instance as the protected-instance of the ERPS ring instance by using command **set protocols erps ring** <*ring-id*> **instance** <*instance-id*> **protected-instance** <*msti*>.

The control VLAN and data VLAN must be configured in the protected instance, only then the ERPS protocol can process messages of these VLANs.

> **NOTE**:
>
> When users want to share the forwarding path of data traffic between intersecting rings, it is important to note that when configuring ERPS, the control VLAN and data VLAN of the intersecting rings should be configured in the same protected instance.
>
> For example, let's assume that two intersecting rings with different control VLANs (such as VLAN 200, VLAN 300), and they share the same data VLAN (such as VLAN 100), it's necessary to configure the control VLANs and data VLAN (VLAN 100, VLAN 200, VLAN 300) into the same protected instance to enable data forwarding between the intersecting rings.
>
> You can refer to Example for Configuring ERPS (Intersection Rings) for detailed configuration.

ERPS Timer

There are three timers used in ERPS protocol: Guard Timer, WTR (Wait to Restore) Timer and Holdoff Timer.

- Guard Timer

The device involved in the signal failure (SF) sends R-APS (NR) messages to other nodes after the failure is recovered or the clearing of SF condition operation is detected. The guard timer is started at the same time, and the R-APS (NR) messages are not processed until this timer expires, with the purpose of preventing the reception of outdated R-APS (NR) messages. If R-APS (NR) messages from other ports are still received after the guard timer expired, the state of this port is changed to Forwarding state.

The guard timer can be configured. The default time interval is 500 milliseconds; the time interval ranges from 10 to 2000 milliseconds.

- Wait-to-Restore (WTR) Timer

When recovering from a signal failure (SF) condition, the WTR timer is used to prevent frequent operation of protection switching due to intermittent SF defects.

The WTR timer can be configured. The delay timer must be long enough to allow the recovering network to become stable. The default time interval is 5 minutes; the time interval ranges from 1 to 12 minutes.

- Holdoff Timer

If the holdoff timer is specified, a defect is not reported to the ring protection mechanism immediately. Instead, the hold-off timer is started. On expiration of the timer, if the defect still exists, it is reported to protection switching.

The holdoff timer can be configured. The default time interval is 0 millisecond; the time interval ranges from 0 to 1000 milliseconds.

- WTB timer

When clearing the forced switching or manual switching state of a port, WTB timer is started. As there may be multiple manually switching blocking nodes in a ERPS ring, and the clearing operation works only when the WTB timer expires, which prevents blocking-point oscillations caused by immediate blocking of the RPL owner port.

WTB Timer cannot be configured directly via CLI, it obtains from the configuration of Guard Timer value plus 5 seconds. The default value is 7 seconds.

Revertive/Non-revertive Mode

ERPS revertive/non-revertive mode determines whether the RPL owner port is re-blocked when the failed link recovers.

- In **revertive mode**, if the failed link recovers, the RPL owner port is re-blocked after waiting for the WTR timer interval. The RPL link is reverted to
- In **non-revertive mode**, if the failed link recovers, the WTR timer is not started, and the blocking link remains on the original failed link and does not revert to RPL link.

By default, the ERPS ring is in revertive mode.

ERPSv2 supports the configuration of revertive and non-revertive modes, while ERPSv1 supports only revertive mode.

Port Blocking Switching Method

Since the RPL link may have higher bandwidth, users can consider blocking the link with low bandwidth to allow data traffic to transmit through the RPL link.

ERPS supports two switching methods to manually configure port blocking: Force Switch and Manual Switch.

- **Forced Switch**: Ports configured for forced switch are blocked immediately, regardless of whether other links on the ring are faulty or not.
- **Manual Switch**: Ports configured for manual switch are blocked if the state of the ring is Idle or Pending, otherwise they are not blocked.

In addition to forced switch and manual switch, ERPS also supports clear operation, which is used in the following three cases:

- Clearing the locally configured manual switch and forced switch configurations.
- When the ERPS ring is in the revertive mode, the revert action is triggered manually before the WTB Timer or WTR Timer expires.
- When the ERPS ring is in non-revertive mode, the revert action is triggered manually.

Users can use the **run show erps ring** <*ring-id*> [**instance** <*instance-id*>] command to view the detailed information of the ERPS ring instances. If force switch (or manual switch) is set successfully, the ***Node state*** in the show result displays **Forced Switch** (or **Manual Switch**).

```
admin@PICOS# run show erps ring 1
Ring ID: 1
Port0: te-1/1/19
```

```
Port1: te-1/1/7
Ring-MAC: false
Sub-ring: No
Virtual-channel: No

Instance ID: 1
Enable: Yes
Active: true
Node state: Forced Switch
Description:
Control VLAN: 4001
Protected instance: 1
Protected VLAN: 100-101,111,4094
……
```

Port blocking manual switching is an ERPSv2 feature which is not supported in ERPSv1.

Virtual-Channel Sub-ring RAPS Message Transmission Method

When ERPS protocol is deployed in multi-ring networking, the transmission methods of RAPS messages on sub-ring nodes are categorized into **Virtual-Channel (VC)** and **Non-Virtual-Channel (NVC)**.

For Virtual-Channel method, the RAPS protocol messages of the sub-ring will transmit in the major ring through the intersecting node. That is, the intersecting node does not terminate the protocol messages of the sub-ring. In this topology, the RPL owner port of the sub-ring blocks both RAPS protocol messages and data traffic of the sub-ring.

R-APS messages from sub-rings are forwarded over virtual channels to be broadcast or multicast over the interconnected network.

R-APS messages forwarded by a sub-ring over a virtual channel need to be distinguishable from R-APS messages of other rings, which can be achieved by using separate control VLANs for the R-APS virtual channels of different sub-rings.

To enable Virtual-Channel method, the following configurations are required:

1. Enable virtual channel on all the devices of the sub-ring, where the *<ring-id>* is the sub-ring ID.

   set protocols erps ring *<ring-id>* **virtual-channel** <**true | false**>

2. Add the ports of major ring, which are used for forwarding R-APS messages from the sub-ring, to the control VLAN of the sub-ring.

Non-Virtual-Channel Sub-ring RAPS Message Transmission Method

For Non-Virtual-Channel method, the RAPS protocol messages of the sub-ring will terminate on the intersecting node, and the RPL owner port of the sub-ring will block only the data traffic but not the RAPS protocol messages of the sub-ring.

If link failure occurs on any link of the sub-ring, the RAPS channel of the sub-ring may be segmented, which prevents RAPS messages from being exchanged between sub-ring links.

By default, the sub-ring RAPS message is transmitted with non-virtual channel method.

Connect Ring for Sub-ring

On a multi-ring network, associate a ring (this is the connect ring, e.g. ring A) with a sub-ring (e.g. sub-ring B) if you want to advertise topology changes in the sub-ring (sub-ring B) to the ring (ring A).

Before using the tcn-propagation function to forward a topology change notification to the connect ring whenever the topology of the sub-ring changed, you need to configure connect ring for the sub-ring. By default, a sub-ring has no connect ring.

Tcn-propagation

Tcn-propagation (topology change notification propagation) function enables sub-ring topology change notifications. When the topology of the sub-ring changes, the FDB refresh of the port will generate a Topology Change (TC) signal. When the tcn-propagation function is enabled, the intersecting node sends an event flush message to the connect ring when it receives the TC signal.

By default, this feature is disabled.

To enable sub-ring topology change notifications, the following configurations are required:

1. Configure the connect ring for a sub-ring on all intersecting nodes.

   set protocols erps ring *<ring-id>* **instance** *<instance-id>* **connect ring** *<ring-id>* **instance** *<instance-id>*

2. Enable tcn-propagation function to advertise topology changes to the connect ring on all intersecting nodes.

   set protocols erps tcn-propagation <**true | false**>

ERPS Operation Mechanism

In normal condition, the communication is normal between devices on the loop, all ports can forward traffic normally except the RPL owner port is blocked by ERPS to prevent network loops. When link failure occurs, there are two ERPS operation process involved: **Link Failure** and **Recovery of Link Failure**, which are described below.

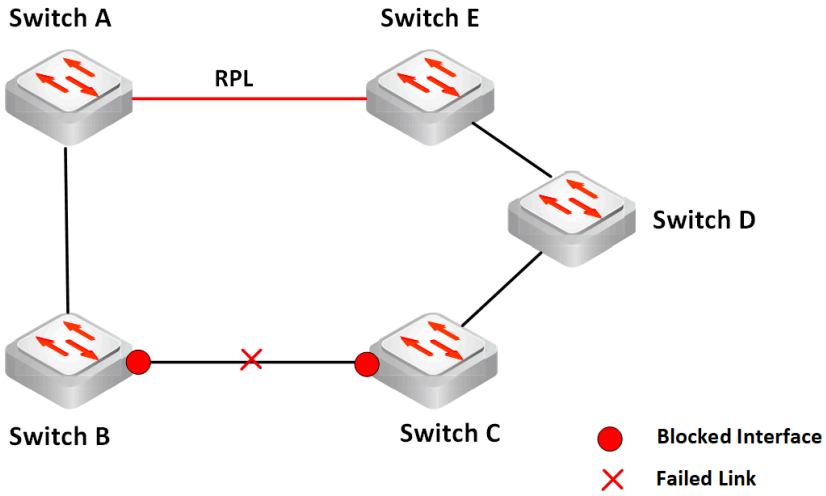
Link Failure

As shown in **Figure 3**, when the link between Switch B and Switch C fails, the ERPS protocol initiates a protection reversal mechanism to block the ports at both ends of the failed link, and then unblocks the RPL owner port, which resumes receiving and sending user traffic, thus ensuring uninterrupted traffic. The detailed process is as follows:

1. Switch B and Switch C detect a link failure, block the port on the failed link, and perform the FDB flush.

2. Switch B and Switch C then start sending R-APS (SF) messages periodically with the (node ID, BPR) pair on both ring ports, while the SF condition persists.
3. When the other devices receive the R-APS (SF) message from Switch B and Switch C, they all perform the FDB flush. When Switch A device (the device where the RPL owner port is located) receives this RAPS message, it unblocks the RPL owner port and RPL neighbor port, performs the FDB flush.

Figure 3. ERPS Link Failure



Recovery of Link Failure

After the link has been recovered from the failure, it can be used to transmit user traffic again, and the RPL owner port will be blocked again. The detailed recovery process is as follows:

1. When the link between Switch B and Switch C is recovered, Switch B and Switch C start a Guard Timer to prevent reception of outdated R-APS (NR) messages, and do not receive other R-APS protocol messages until the timer expires. At the same time Switch B and Switch C sends R-APS (NR) messages to other nodes.
2. When Switch A (the device where the RPL owner port is located) receives the R-APS (NR) message, it starts the WTR Timer. On expiration of the WTR timer, the RPL owner node blocks its end of the RPL, sends an R-APS (NR, RB) message with the (node ID, BPR) pair and performs the FDB flush.
3. When Switch B and Switch C receive the NR-RB (No request, RPL block) R-APS message from Switch A, they remove the block on its blocked ring ports, stop sending R-APS (NR) messages and perform the FDB flush. In addition to this, ethernet ring nodes B to E perform the FDB flush when receiving an R-APS (NR, RB) message due to the node ID and BPR-based mechanism.

Configuration Notes and Constraints of ERPS

When configuring ERPS, consider the following points:

- A maximum of eight ERPS rings (including both major ring and sub-ring) are supported on a device, and a maximum of two instances can be configured for each ring.
- The ERPS port must be a trunk port.
- Before enabling ERPS, users need to disable spanning tree protocol on specific port.
- Traffic from VLANs other than the control VLAN or data VLAN will be dropped by the ERPS ports.
- Make sure that the control VLAN and data VLANs of an ERPS ring have all been added to the MSTP instance (ERPS protected-instance) and VLAN
- When the ERPS ring instance is enabled, the traffic of MSTP instance 0 will be blocked.
- Control VLAN should be assigned as a tagged VLAN.
- Different ERPS ring instances cannot use the same control VLAN.
- The same control VLAN must be configured for all devices in the same ERPS ring instance.
- To ensure the fast convergence of ERPS, it is recommended not to configure the intersecting link as an RPL link in the configuration of the intersecting ring.
- ERPS only works with MSTP, but not STP/RSTP/PVST.
- MLAG configuration on ERPS ring ports is not supported.
- On such deployments, where gateways are serving VLANs across the ring, VRRP is recommended.

Configuring ERPS

PICOS supports both versions of ERPSv1 and ERPSv2. ERPSv2 is fully compatible with ERPSv1 and has the following extensions:

- Sub-ring supporting
- Sub-ring virtual channel/non-virtual channel transmission of RAPS messages
- Manual switching of port blocking, including Forced Switch and Manual Switch
- ERPS ring revertive/non-revertive modes are configurable
- Sub-ring topology change notifications

Procedure

Step1 Disable spanning-tree protocol on the interface where you want to enable ERPS.

set protocols spanning-tree interface <*interface-name*> **enable false**

Step2 Configure protected MSTP instance (i.e., ERPS protected-instance) and VLAN mapping before configuring ERPS. The ERPS control VLAN must be in one of the protected-msti.

set protocols spanning-tree mstp msti <*msti*> **vlan** <*vlan-id*>

Step3 Configure the port mode to **trunk**, configure VLAN member.

NOTEs:

- Both the control VLAN and data VLAN have to be configured as the VLAN member of the ERPS port.
- Control VLAN should be assigned as a tagged VLAN. If not explicitly specified, VLAN is tagged in VLAN member configuration by default.

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching port-mode** <*port-mode*>

set interface gigabit-ethernet <*interface-name*> **family ethernet-switching vlan members** <*vlan-id*>

Step4 Enable ERPS function globally. By default, ERPS is disabled.

set protocols erps enable <**true | false**>

Step5 (Optional) Configure ERPS version. The default version is ERPSv2.

set protocols erps version <1 | 2>

Step6 Create an ERPS ring with a given ID. By default, ERPS ring is a major ring. A maximum of eight ERPS rings are supported on a device.

set protocols erps ring <*ring-id*>

Step7 (Optional) Create an ERPS sub-ring with a given ID.

set protocols erps ring <*ring-id*> **sub-ring** <**true | false**>

Step8 Configure ERPS ring ports: port0 and port1.

set protocols erps ring <*ring-id*> **port0 interface** <*interface-name*>

set protocols erps ring <*ring-id*> **port1 interface** <*interface-name*>

Step9 Create an instance for the ERPS ring. A maximum of two instances can be configured for each ring.

set protocols erps ring <*ring-id*> **instance** <**1** | **2**>

Step10 Configure RPL port role for the ERPS ring instance. Each ERPS ring instance has only one RPL owner port and neighbor port.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **rpl** <**port0** | **port1**> <**owner** | **neighbor**>

Step11 Configure a control VLAN. Note that the same control VLAN must be configured for all devices in the same ERPS ring instance.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **control-vlan** <*control-vlan*>

Step12 Configure the MSTP instance of VLANs that are protected by the ERPS ring instance.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **protected-instance** <*msti*>

Step13 (Optional) Configure the guard timer, holdoff timer and WTR timer duration for a ring instance.

By default, guard timer is 500 milliseconds, holdoff timer is 0 millisecond and WTR timer is 5 minutes.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **guard-timer** <*guard-timer*>

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **holdoff-timer** <*holdoff-timer*>

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **wtr-timer** <*wtr-timer*>

Step14 (Optional) Configure the ring ID as the last byte of the destination MAC address for R-APS packets.

set protocols erps ring <*ring-id*> **r-aps ring-mac**

Step15 (Optional) Configure the Automatic Protection Switching (APS) message level for the node on the Ethernet ring.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **r-aps level** <*level-id*>

Step16 (Optional) Configure ERPS revertive/non-revertive mode. By default, the ERPS ring is in revertive mode.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **non-revertive** <**true | false**>

Step17 (Optional) Configure virtual-channel sub-ring RAPS message transmission method. By default, the sub-ring RAPS message is transmitted with the non-virtual channel method.

set protocols erps ring <*ring-id*> **virtual-channel** <**true | false**>

Step18 (Optional) Configure the connect ring for a sub-ring, enable tcn-propagation function to advertise topology changes to the connect ring.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **connect ring** <*ring-id*> **instance** <*instance-id*>

set protocols erps tcn-propagation <**true | false**>

Step19 Commit the configuration.

commit

Step20 (Optional) In operational mode, block a specific ring interface in one of the two following ways:

- Force: The switch blocks a specific ring interface regardless of the protection switching state of the ring instance.
- Manual: The switch blocks a specific ring interface if no other protection switch event is active on the ring instance.

erps switch force ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

erps switch manual ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

erps clear ring <*ring-id*> **instance** <*instance-id*>

Step21 View the configuration information and status of ERPS.

run show erps interface ring <*ring-id*> **instance** <*instance-id*>

run show erps brief

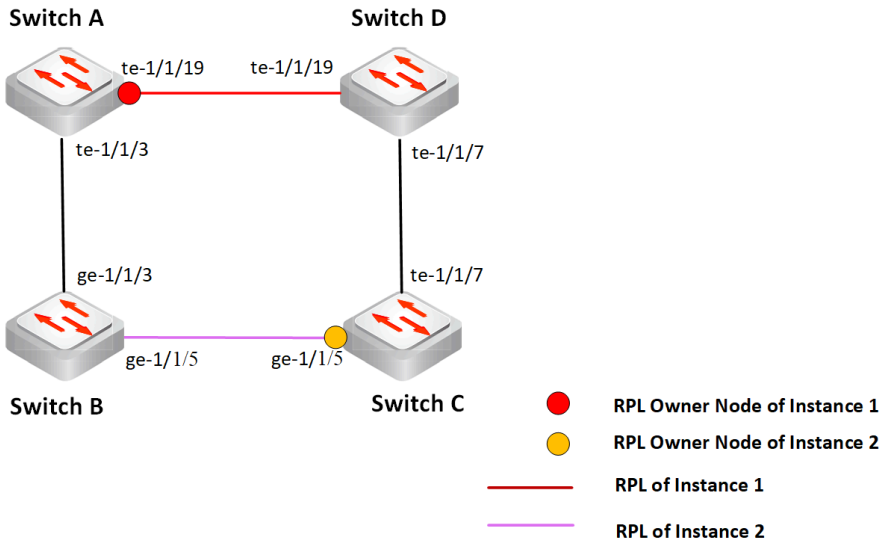
run show erps ring <*ring-id*> [**instance** <*instance-id*>]

Example for Configuring ERPS (Single Ring)

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
  - Verifying the Configuration

Networking Requirements

Figure 1. ERPS Configuration Example



To solve the loop problem caused by redundant links in the network, ERPS protocol can be deployed on the devices that form the ring network. As shown in **Figure 4**, taking the deployment of a single-ring multi-instance ERPS ring as an example.

- Switch A, Switch B, Switch C and Switch D form an ERPS ring, on which two instances are configured.
- The RPL Owner Node of instance 1 is the interface te-1/1/19 (port1) on Switch A. The RPL is the link between Switch A and Switch D. The control VLAN is VLAN 4001 and the data VLANs are VLAN 100-200.
- The RPL Owner Node of instance 2 is the interface ge-1/1/5 (port0) on Switch C. Its RPL is the link between Switch B and Switch C. The control VLAN is VLAN 4002 and the data VLANs are VLANs 300-400.

NOTEs:

- The ERPS port must be a trunk port and disable spanning tree protocol.
- Different ERPS ring instances cannot use the same control VLAN.
- The same control VLAN must be configured for all devices in the same ERPS ring instance.

Procedure

Switch A

Step1 Disable spanning-tree protocol on the interface where you want to enable ERPS.

```
admin@SwitchA# set protocols spanning-tree interface te-1/1/3 enable false
admin@SwitchA# set protocols spanning-tree interface te-1/1/19 enable false
```

Step2 Configure protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchA# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchA# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchA# set protocols spanning-tree mstp msti 2 vlan 300-400
admin@SwitchA# set protocols spanning-tree mstp msti 2 vlan 4002
```

Step3 Configure VLAN and port mode.

```
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 100-200,300-400,4001
admin@SwitchA# set interface gigabit-ethernet te-1/1/19 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/19 family ethernet-switching vlan members 100-200,300-400,400
```

Step4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchA# set protocols erps enable true
```

Step5 Create the ERPS ring with a given ID.

```
admin@SwitchA# set protocols erps ring 1
```

Step6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchA# set protocols erps ring 1 port0 interface te-1/1/3
admin@SwitchA# set protocols erps ring 1 port1 interface te-1/1/19
```

Step7 Create instance for the ERPS ring.

```
admin@SwitchA# set protocols erps ring 1 instance 1
admin@SwitchA# set protocols erps ring 1 instance 2
```

Step8 Configure port te-1/1/19 (port1) on Switch A as the RPL Owner Node for ERPS ring 1 instance 1.

```
admin@SwitchA# set protocols erps ring 1 instance 1 rpl port1 owner
```

Step9 Configure the control VLAN.

```
admin@SwitchA# set protocols erps ring 1 instance 1 control-vlan 4001
admin@SwitchA# set protocols erps ring 1 instance 2 control-vlan 4002
```

Step10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchA# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchA# set protocols erps ring 1 instance 2 protected-instance 2
```

Step11 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Disable spanning-tree protocol on the interface where you want to enable ERPS.

```
admin@SwitchB# set protocols spanning-tree interface ge-1/1/3 enable false
admin@SwitchB# set protocols spanning-tree interface ge-1/1/5 enable false
```

Step2 Configure protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchB# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchB# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchB# set protocols spanning-tree mstp msti 2 vlan 300-400
admin@SwitchB# set protocols spanning-tree mstp msti 2 vlan 4002
```

Step3 Configure VLAN and port mode.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100-200,300-400,4001
admin@SwitchB# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 100-200,300-400,4001
```

Step4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchB# set protocols erps enable true
```

Step5 Create the ERPS ring with a given ID.

```
admin@SwitchB# set protocols erps ring 1
```

Step6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchB# set protocols erps ring 1 port0 interface ge-1/1/3
admin@SwitchB# set protocols erps ring 1 port1 interface ge-1/1/5
```

Step7 Create instance for the ERPS ring.

```
admin@SwitchB# set protocols erps ring 1 instance 1
admin@SwitchB# set protocols erps ring 1 instance 2
```

Step8 Configure port ge-1/1/5 (port1) on Switch C as the RPL Neighbor Node for ERPS ring 1 instance 2.

```
admin@SwitchB# set protocols erps ring 1 instance 2 rpl port1 neighbor
```

Step9 Configure the control VLAN.

```
admin@SwitchB# set protocols erps ring 1 instance 1 control-vlan 4001
admin@SwitchB# set protocols erps ring 1 instance 2 control-vlan 4002
```

Step10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchB# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchB# set protocols erps ring 1 instance 2 protected-instance 2
```

Step11 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Disable spanning-tree protocol on the interface where you want to enable ERPS.

```
admin@SwitchC# set protocols spanning-tree interface te-1/1/7 enable false
admin@SwitchC# set protocols spanning-tree interface ge-1/1/5 enable false
```

Step2 Configure MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchC# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchC# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchC# set protocols spanning-tree mstp msti 2 vlan 300-400
admin@SwitchC# set protocols spanning-tree mstp msti 2 vlan 4002
```

Step3 Configure VLAN and port mode.

```
admin@SwitchC# set interface gigabit-ethernet te-1/1/7 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet te-1/1/7 family ethernet-switching vlan members 100-200,300-400,4001
admin@SwitchC# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 100-200,300-400,4001
```

Step4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchC# set protocols erps enable true
```

Step5 Create the ERPS ring with a given ID.

```
admin@SwitchC# set protocols erps ring 1
```

Step6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchC# set protocols erps ring 1 port0 interface ge-1/1/5
admin@SwitchC# set protocols erps ring 1 port1 interface te-1/1/7
```

Step7 Create instance for the ERPS ring.

```
admin@SwitchC# set protocols erps ring 1 instance 1
admin@SwitchC# set protocols erps ring 1 instance 2
```

Step8 Configure port ge-1/1/5 (port0) on Switch C as the RPL Owner Node for ERPS ring 1 instance 2.

```
admin@SwitchC# set protocols erps ring 1 instance 2 rpl port0 owner
```

Step9 Configure the control VLAN.

```
admin@SwitchC# set protocols erps ring 1 instance 1 control-vlan 4001
admin@SwitchC# set protocols erps ring 1 instance 2 control-vlan 4002
```

Step10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchC# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchC# set protocols erps ring 1 instance 2 protected-instance 2
```

Step11 Commit the configurations.

```
admin@SwitchC# commit
```

Switch D

Step1 Disable spanning-tree protocol on the interface where you want to enable ERPS.

```
admin@SwitchD# set protocols spanning-tree interface te-1/1/7 enable false
admin@SwitchD# set protocols spanning-tree interface te-1/1/19 enable false
```

Step2 Configure the protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchD# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchD# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchD# set protocols spanning-tree mstp msti 2 vlan 300-400
admin@SwitchD# set protocols spanning-tree mstp msti 2 vlan 4002
```

Step3 Configure VLAN and port mode.

```
admin@SwitchD# set interface gigabit-ethernet te-1/1/7 family ethernet-switching port-mode trunk
admin@SwitchD# set interface gigabit-ethernet te-1/1/7 family ethernet-switching vlan members 100-200,300-400,4001
admin@SwitchD# set interface gigabit-ethernet te-1/1/19 family ethernet-switching port-mode trunk
admin@SwitchD# set interface gigabit-ethernet te-1/1/19 family ethernet-switching vlan members 100-200,300-400,400
```

Step4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchD# set protocols erps enable true
```

Step5 Create the ERPS ring with a given ID.

```
admin@SwitchD# set protocols erps ring 1
```

Step6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchD# set protocols erps ring 1 port0 interface te-1/1/7
```

```
admin@SwitchD# set protocols erps ring 1 port1 interface te-1/1/19
```

Step7 Create instance for the ERPS ring.

```
admin@SwitchD# set protocols erps ring 1 instance 1
admin@SwitchD# set protocols erps ring 1 instance 2
```

Step8 Configure port te-1/1/19 (port1) on Switch D as the RPL Neighbor port for ERPS ring 1 instance 1.

```
admin@SwitchD# set protocols erps ring 1 instance 1 rpl port1 neighbor
```

Step9 Configure the control VLAN.

```
admin@SwitchD# set protocols erps ring 1 instance 1 control-vlan 4001
admin@SwitchD# set protocols erps ring 1 instance 2 control-vlan 4002
```

Step10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchD# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchD# set protocols erps ring 1 instance 2 protected-instance 2
```

Step11 Commit the configurations.

```
admin@SwitchD# commit
```

Verifying the Configuration

- The command **run show erps brief** can be used to check the brief configuration information of the ERPS ring. Take Switch A as an example:

```
admin@SwitchA# run show erps brief
Enable: true
Version: 2
Tcn-propagation: No

D: Discarding
F: Forwarding
R: RPL Owner
N: RPL Neighbour
FS: Forced Switch
MS: Manual Switch
Ring ID    Instance ID    Control VLAN    Port0            Port1
------------------------------------------------------------------------------
1          1              4001            te-1/1/3(F)      te-1/1/19 (D,R)
1          2              4002            te-1/1/3(F)      te-1/1/19(F)
```

- The command **run show erps ring** *<ring-id>* can be used to check the detailed information of the ERPS ring. Take Switch A as an example:

```
admin@SwitchA# run show erps ring 1
Ring ID: 1
Port0: te-1/1/3
Port1: te-1/1/19
Ring-MAC: false
Sub-ring: No
Virtual-channel: No

Instance ID: 1
Enable: Yes
Active: true
Node state: Idle
Description:
Control VLAN: 4001
Protected instance: 1
Protected VLAN: 100-200
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 5 min
Revertive mode: Revertive
```

```
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role      Port State       Signal Failure
--------------------------------------------------------------------------------
te-1/1/3       Common         Forwarding     Non-failed
te-1/1/19      RPL Owner      Discarding      Non-failed

Instance ID: 2
Enable: Yes
Active: true
Node state: Idle
Description:
Control VLAN: 4002
Protected instance: 2
Protected VLAN: 300-400
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 5 min
Revertive mode: Revertive
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role      Port State       Signal Failure
------------------------------------------------------------------
te-1/1/3       Common         Forwarding       Non-failed
te-1/1/19      Common         Forwarding       Non-failed
```

From the show result, we can see that port te-1/1/19 on Switch A is the Owner node in Instance 1, with the ERPS ring in the Idle state, the RPL owner port blocked, and the port state of the non-RPL owner port is forwarding.

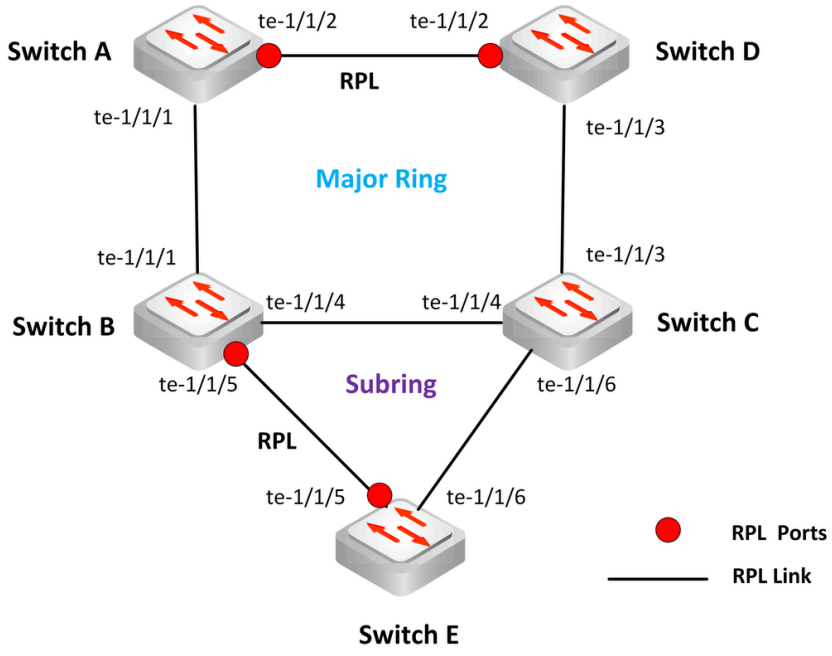
In Instance 2, port0 and port1 are Normal nodes, the ERPS ring is in the Idle state, and the port state of the non-RPL owner ports are forwarding.

Example for Configuring ERPS (Intersection Rings)

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
  - Switch E
- Verifying the Configuration

Networking Requirements

Figure 1. ERPS Configuration Example



To solve the loop problem caused by redundant links in the network, ERPS protocol can be deployed on the devices that form the ring network. As shown in **Figure 1**, taking the deployment of the interconnection ERPS ring as an example.

- Switch A, Switch B, Switch C and Switch D form an ERPS major ring, ring ID is 1 and protected instance is 1; Switch B, Switch C and Switch E form a sub-ring, ring ID is 2 and protected instance is 2.
- Configure the control VLAN ID of ERPS ring 1 to be 4001 and the control VLAN ID of ERPS ring 2 to be 4002. ERPS ring 1 and ring 2 transmit data packets for the same user VLAN 100 to 200.
- Users wish to share the forwarding path between the intersecting rings for the data traffic, in such case, it is necessary to configure the control VLANs and data VLANs (VLAN 4001, 4002, 100 to 200) into the same protected instance to achieve data forwarding between the intersecting rings.
- Configure network topology change notification on intersecting nodes Switch B and Switch C. The following configurations are required:

  1. Configure the connect ring for a sub-ring on all intersecting nodes.

  set protocols erps ring <*ring-id*> **instance** <*instance-id*> **connect ring** <*ring-id*> **instance** <*instance-id*>

  2. Enable tcn-propagation function to advertise topology changes to the connect ring on all intersecting nodes.

set protocols erps tcn-propagation <**true | false**>

NOTEs:

- The ERPS port must be a trunk port and disable spanning tree protocol.
- Different ERPS ring instances cannot use the same control VLAN.
- The same control VLAN must be configured for all devices in the same ERPS ring instance.

Procedure

Switch A

Step 1 Disable spanning-tree protocol on the interface before configuring ERPS ring on the interface.

```
admin@SwitchA# set protocols spanning-tree interface te-1/1/1 enable false
admin@SwitchA# set protocols spanning-tree interface te-1/1/2 enable false
```

Step 2 Configure protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchA# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchA# set protocols spanning-tree mstp msti 1 vlan 4001
```

Step 3 Configure VLAN and port mode.

```
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 100-200,4001
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 100-200,4001
```

Step 4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchA# set protocols erps enable true
```

Step 5 Create the ERPS ring with a given ID.

```
admin@SwitchA# set protocols erps ring 1
```

Step 6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchA# set protocols erps ring 1 port0 interface te-1/1/1
admin@SwitchA# set protocols erps ring 1 port1 interface te-1/1/2
```

Step 7 Create instance for the ERPS ring.

```
admin@SwitchA# set protocols erps ring 1 instance 1
```

Step 8 Configure port te-1/1/2 (port1) on Switch A as the RPL Owner Node for ERPS ring 1 instance 1.

```
admin@SwitchA# set protocols erps ring 1 instance 1 rpl port1 owner
```

Step 9 Configure the control VLAN.

```
admin@SwitchA# set protocols erps ring 1 instance 1 control-vlan 4001
```

Step 10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchA# set protocols erps ring 1 instance 1 protected-instance 1
```

Step 11 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step 1 Disable spanning-tree protocol on the interface before configuring ERPS ring on the interface.

```
admin@SwitchB# set protocols spanning-tree interface te-1/1/1 enable false
admin@SwitchB# set protocols spanning-tree interface te-1/1/4 enable false
admin@SwitchB# set protocols spanning-tree interface te-1/1/5 enable false
```

Step 2 Configure protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: Configure the control VLAN and data VLAN of ring 1 and ring 2 (VLAN 4001, 4002, 100 to 200) into the same protected instance to achieve data forwarding between the intersecting rings.

```
admin@SwitchB# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchB# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchB# set protocols spanning-tree mstp msti 1 vlan 4002
```

Step 3 Configure VLAN and port mode.

```
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 100-200,4001
admin@SwitchB# set interface gigabit-ethernet te-1/1/4 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/4 family ethernet-switching vlan members 100-200,4001
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching vlan members 100-200,4002
```

Step 4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchB# set protocols erps enable true
```

Step 5 Create the ERPS ring 1 and 2, and specify ring 2 as a sub-ring.

```
admin@SwitchB# set protocols erps ring 1
admin@SwitchB# set protocols erps ring 2 sub-ring true
```

Step 6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchB# set protocols erps ring 1 port0 interface te-1/1/1
admin@SwitchB# set protocols erps ring 1 port1 interface te-1/1/4
admin@SwitchB# set protocols erps ring 2 port0 interface te-1/1/5
```

Step 7 Configure port te-1/1/5 (port0) on Switch B as the RPL Owner Node for ERPS ring 2 instance 2.

```
admin@SwitchB# set protocols erps ring 2 instance 2 rpl port0 owner
```

Step 8 Create instance for the ERPS ring.

```
admin@SwitchB# set protocols erps ring 1 instance 1
admin@SwitchB# set protocols erps ring 2 instance 2
```

Step 9 Configure the control VLAN.

```
admin@SwitchB# set protocols erps ring 1 instance 1 control-vlan 4001
```

```
admin@SwitchB# set protocols erps ring 2 instance 2 control-vlan 4002
```

Step 10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchB# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchB# set protocols erps ring 2 instance 2 protected-instance 1
```

Step 11 Configure the connect ring for sub-ring 2, and enable network topology change notification on intersecting nodes Switch B and Switch C.

```
admin@SwitchB# set protocols erps ring 2 instance 2 connect ring 1 instance 1
admin@SwitchB# set protocols erps tcn-propagation true
```

Step 12 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step 1 Disable spanning-tree protocol on the interface before configuring ERPS ring on the interface.

```
admin@SwitchC# set protocols spanning-tree interface te-1/1/3 enable false
admin@SwitchC# set protocols spanning-tree interface te-1/1/4 enable false
admin@SwitchC# set protocols spanning-tree interface te-1/1/6 enable false
```

Step 2 Configure MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: Configure the control VLAN and data VLAN of ring 1 and ring 2 (VLAN 4001, 4002, 100 to 200) into the same protected instance to enable data forwarding between the intersecting rings.

```
admin@SwitchC# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchC# set protocols spanning-tree mstp msti 1 vlan 4001
admin@SwitchC# set protocols spanning-tree mstp msti 1 vlan 4002
```

Step 3 Configure VLAN and port mode.

```
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 100-200,4001
admin@SwitchC# set interface gigabit-ethernet te-1/1/4 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet te-1/1/4 family ethernet-switching vlan members 100-200,4001
admin@SwitchC# set interface gigabit-ethernet te-1/1/6 family ethernet-switching port-mode trunk
admin@SwitchC# set interface gigabit-ethernet te-1/1/6 family ethernet-switching vlan members 100-200,4002
```

Step 4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchC# set protocols erps enable true
```

Step 5 Create the ERPS ring with a given ID.

```
admin@SwitchC# set protocols erps ring 1
admin@SwitchC# set protocols erps ring 2 sub-ring true
```

Step 6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchC# set protocols erps ring 1 port0 interface te-1/1/3
admin@SwitchC# set protocols erps ring 1 port1 interface te-1/1/4
admin@SwitchC# set protocols erps ring 2 port0 interface te-1/1/6
```

Step 7 Create instance for the ERPS ring.

```
admin@SwitchC# set protocols erps ring 1 instance 1
admin@SwitchC# set protocols erps ring 2 instance 2
```

Step 8 Configure the control VLAN.

```
admin@SwitchC# set protocols erps ring 1 instance 1 control-vlan 4001
admin@SwitchC# set protocols erps ring 2 instance 2 control-vlan 4002
```

Step 9 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchC# set protocols erps ring 1 instance 1 protected-instance 1
admin@SwitchC# set protocols erps ring 2 instance 2 protected-instance 1
```

Step 10 Configure the connect ring for sub-ring 2, and enable network topology change notification on intersecting nodes Switch B and Switch C.

```
admin@SwitchC# set protocols erps ring 2 instance 2 connect ring 1 instance 1
admin@SwitchC# set protocols erps tcn-propagation true
```

Step 11 Commit the configurations.

```
admin@SwitchC# commit
```

Switch D

Step 1 Disable spanning-tree protocol on the interface before configuring ERPS ring on the interface.

```
admin@SwitchD# set protocols spanning-tree interface te-1/1/2 enable false
admin@SwitchD# set protocols spanning-tree interface te-1/1/3 enable false
```

Step 2 Configure the protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

NOTE: The ERPS control VLAN must be in one of the protected MSTP instance.

```
admin@SwitchD# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchD# set protocols spanning-tree mstp msti 1 vlan 4001
```

Step 3 Configure VLAN and port mode.

```
admin@SwitchD# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchD# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 100-200,4001
admin@SwitchD# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@SwitchD# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 100-200,4001
```

Step 4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchD# set protocols erps enable true
```

Step 5 Create the ERPS ring with a given ID.

```
admin@SwitchD# set protocols erps ring 1
```

Step 6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchD# set protocols erps ring 1 port0 interface te-1/1/2
admin@SwitchD# set protocols erps ring 1 port1 interface te-1/1/3
```

Step 7 Create instance for the ERPS ring.

```
admin@SwitchD# set protocols erps ring 1 instance 1
```

Step 8 Configure port te-1/1/2 (port0) on Switch D as the RPL Neighbor port for the ERPS ring 1 instance 1.

```
admin@SwitchD# set protocols erps ring 1 instance 1 rpl port0 neighbor
```

Step 9 Configure the control VLAN.

```
admin@SwitchD# set protocols erps ring 1 instance 1 control-vlan 4001
```

Step 10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchD# set protocols erps ring 1 instance 1 protected-instance 1
```

Step 11 Commit the configurations.

```
admin@SwitchD# commit
```

Switch E

Step 1 Disable spanning-tree protocol on the interface before configuring ERPS ring on the interface.

```
admin@SwitchE# set protocols spanning-tree interface te-1/1/5 enable false
admin@SwitchE# set protocols spanning-tree interface te-1/1/6 enable false
```

Step 2 Configure the protected MSTP instance (ERPS protected-instance) and VLAN mapping before configuring ERPS.

```
admin@SwitchE# set protocols spanning-tree mstp msti 1 vlan 100-200
admin@SwitchE# set protocols spanning-tree mstp msti 1 vlan 4002
```

Step 3 Configure VLAN and port mode.

```
admin@SwitchE# set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode trunk
admin@SwitchE# set interface gigabit-ethernet te-1/1/5 family ethernet-switching vlan members 100-200,4002
admin@SwitchE# set interface gigabit-ethernet te-1/1/6 family ethernet-switching port-mode trunk
admin@SwitchE# set interface gigabit-ethernet te-1/1/6 family ethernet-switching vlan members 100-200,4002
```

Step 4 Enable ERPS function globally. By default, ERPS is disabled.

```
admin@SwitchE# set protocols erps enable true
```

Step 5 Create the ERPS ring with a given ID.

```
admin@SwitchE# set protocols erps ring 2 sub-ring true
```

Step 6 Configure port0 and port1 of the ERPS ring.

```
admin@SwitchE# set protocols erps ring 2 port0 interface te-1/1/5
admin@SwitchE# set protocols erps ring 2 port1 interface te-1/1/6
```

Step 7 Create instance for the ERPS ring.

```
admin@SwitchE# set protocols erps ring 2 instance 2
```

Step 8 Configure port te-1/1/5 (port0) on Switch D as the RPL Neighbor port for the ERPS ring 2 instance 2.

```
admin@SwitchE# set protocols erps ring 2 instance 2 rpl port0 neighbor
```

Step 9 Configure the control VLAN.

```
admin@SwitchE# set protocols erps ring 2 instance 2 control-vlan 4002
```

Step 10 Configure the MSTP instance of VLANs that are protected by this ring instance.

```
admin@SwitchE# set protocols erps ring 2 instance 2 protected-instance 1
```

Step 11 Commit the configurations.

```
admin@SwitchE# commit
```

Verifying the Configuration

- The command **run show erps brief** can be used to check the brief configuration information of the ERPS ring. Take Switch A and Switch B as an example:

```
admin@SwitchA# run show erps brief
Enable: true
Version: 2
Tcn-propagation: No

D: Discarding
F: Forwarding
R: RPL Owner
N: RPL Neighbour
FS: Forced Switch
MS: Manual Switch
Ring ID    Instance ID    Control VLAN      Port0           Port1
------------------------------------------------------------------------------
1               1           4001            te-1/1/1(F)     te-1/1/2 (D,R)


admin@SwitchB# run show erps brief
Enable: Yes
Version: 2
Tcn-propagation: Yes

D: Discarding
F: Forwarding
R: RPL Owner
N: RPL Neighbour
FS: Forced Switch
MS: Manual Switch
Ring ID       Instance ID        Control VLAN      Port0               Port1
-------       -----------       ------------       -----------------   -----------------
1               1                 4001             te-1/1/1(F)         te-1/1/4 (D,R)
2               2                 4002             te-1/1/5(D,R)       -
```

- The command **run show erps ring** *<ring-id>* can be used to check the detailed information of the ERPS ring. Take Switch A as an example:

```
admin@SwitchA# run show erps ring 1
Ring ID: 1
Port0: te-1/1/1
Port1: te-1/1/2
Ring-MAC: false
Sub-ring: No
Virtual-channel: No

Instance ID: 1
Enable: Yes
```

```
Active: true
Node state: Idle
Description:
Control VLAN: 4001
Protected instance: 1
Protected VLAN: 100-200
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 5 min
Revertive mode: Revertive
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role       Port State     Signal Failure
-------------------------------------------------------------
te-1/1/1       Common          Forwarding     Non-failed
te-1/1/2       RPL Owner       Discarding     Non-failed
```

From the show result, we can see that port te-1/1/2 on Switch A is the Owner node in Instance 1, with the ERPS ring in the Idle state, the RPL port blocked, and the non-RPL port state is forwarding.

Loopback Detection

- Overview of Loopback Detection
- Configuring Loopback Detection

Overview of Loopback Detection

Overview
Detection Message
Loopback Detection Action

Overview

Loopback detection is a network technology used to identify and prevent switching loops within a network infrastructure. Switching loops occur when there is more than one path for data to travel between network devices, causing packets to continuously circulate and potentially overwhelm the network.

Loopback detection works by sending loopback detection messages out on interfaces and then monitoring for these messages to return. If the message returns to the originating switch, it indicates that a loop is present.

- If the loopback detection message is received from the sending interface, it is considered that the interface is self-looped or there is a loop in the network connected to the interface.
- If the loopback detection message is received by other interfaces on this device, it is considered that the network where the interface is located has a loop, or the device itself has a self-loop.

If a loop is detected, the switch takes action to mitigate it by disabling the affected interfaces and changing their state to ***err-disable***. This helps maintain network stability and prevents performance degradation caused by excessive traffic looping.

> **NOTE**:
>
> The loopback detection message is sent only on the native VLAN. Upon receiving a loopback detection message, the device checks the source MAC address to determine if the message originated from itself, disregarding the VLAN tag.

Detection Message

The format of loopback detection message is depicted below.

DMAC	SMAC	802.1Q Tag	Protocol-Type	PortIndex

Field	Description
DMAC	The value of the destination MAC address is set to all Fs, regardless of whether the packet is tagged or untagged. This ensures that detection packets can be looped back to the device when a loop occurs on an interface or in the network.
SMAC	The source MAC address is set to the system MAC address of the local device to uniquely identify the packets sent by this device.
802.1Q Tag	It includes the Tag Protocol Identifier (TPID), with a value of 0x8100, indicating an 802.1Q tagged frame.
Protocol-Type	The protocol type field has a value of 0x9000, indicating a loopback detection message.
PortIndex	It represents the interface information of the sender of the detection message, allowing the device to compare interfaces and determine whether the message was sent from one of its own interfaces.

Loopback Detection Action

When the ingress interface receives a Loopback Detection (LBD) message sent from this device, then a loop is detected, the ingress interface will be set to the ***err-disable*** state, causing the physical link to go down. Additionally, the loop information will be logged.

You can clear the ***err-disable*** state of the interface through the following methods:

- Use the command **run clear loopback-detection interface** to clear the ***err-disable*** state of the interface.
- Delete the loopback detection configuration can clear the state of the interface.
- Administratively reset the interface by disabling and then enabling it using the configuration commands.
- Disable the loopback detection protocol to clear the state of the interface.

When loops occur within interfaces or networks, they can negatively impact routine business operations. Loopback detection, as a technology designed for detecting loops at a single node, possesses limited capabilities for resolving such loops. Consequently, it is recommended that users address loop-related problems promptly upon detection.

Configuring Loopback Detection

Configuration Notes and Constraints
Configuring Loopback Detection
Example for Configuring Loopback Detection
Networking Requirements
Procedure

Configuration Notes and Constraints

When configuring loopback detection, consider the following points:

- The loopback detection message is sent in the native VLAN. When a loopback detection message is received, the device considers the source MAC address to determine if the message was sent from this device, without considering the VLAN tag.
- Loopback detection can be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
- To enable the loopback detection function, users need to enable loopback detection BOTH globally and at the per-interface level.
- Loopback detection is not supported in Multi-Chassis Link Aggregation (MLAG) scenarios.

Configuring Loopback Detection

Step 1 Enable loopback detection function globally.

set protocols loopback-detection enable <**true** | **false**>

Step 2 Enable loopback detection function on a specific interface.

set protocols loopback-detection interface <*interface-name*> **enable** <**true** | **false**>

Step 3 (Optional) Configure the loopback detection message transmission period.

set protocols loopback-detection message-interval <*message-interval*>

Step 4 (Optional) Clear the ***err-disable*** state of the loopback-detection interface.

run clear loopback-detection interface {<*interface-name*> | **all**}

Step 5 Commit the configuration.

commit

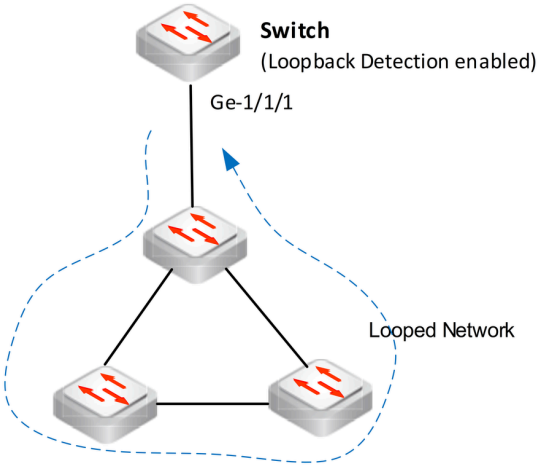
Step 6 View the configuration information and status information of loopback detection.

run show loopback-detection

Example for Configuring Loopback Detection

Networking Requirements

Figure 1. Loopback Detection Configuration Example



As shown in **Figure 1**, if there is a loop in the network connected to interface ge-1/1/1 of the device Switch, it will cause a broadcast storm, and communication on the Switch and the entire network may be affected.

Users hope to detect loops in the downstream network connected to the Switch and reduce the impact of the loop to the networks by blocking the downlink interface. Users can achieve this by enabling loopback detection function on ge-1/1/1 of the Switch. Once a loop is detected, interface state of ge-1/1/1 will be set to ***err-disable***, resulting in the disconnection of the interface. This action helps to reduce the impact of the loop on the device and the network.

Procedure

Step 1 Enable loopback detection function globally.

```
admin@Switch# set protocols loopback-detection enable true
```

Step 2 Enable loopback detection function on a specific interface.

```
admin@Switch# set protocols loopback-detection interface ge-1/1/1 enable true
```

Step 3 Commit the configurations.

```
admin@Switch# commit
```

Step 4 View the configuration information and status information of loopback detection.

```
admin@Switch# run show loopback-detection
Loopback-detection: enabled
message-interval: 30s
Interface       LBD Tx         Status                From_Port
----------      -----------    ------------          -----------
ge-1/1/1        true           LoopDetected          ge-1/1/1
ge-1/1/2        false          Normal
......

admin@Switch# run show interface gigabit-ethernet xe-1/1/1
Physical interface: ge-1/1/1, Enabled, error-discard True(LBD), Physical link is Down
Interface index: 73, QSFP+ type: 40G_BASE_SR4, Mac Learning Enabled
Port mode: access
Description:
…….
```

From the show result, we can see that,

- **Status** of interface ge-1/1/1 is “***LoopDetected***” and “***error-discard True(LBD)***, ***Physical link is Down***”, indicating a loop is detected and the interface is disabled.
- When a loopback is detected, the field **From_Port** indicates the sending interface of loopback detection packets.

Layer 3 Routing Configuration

This chapter describes the configuration steps of Layer 3 routing, including static routing, RIPv2, OSPFv2, VRRP, and ECMP.

- ARP Configuration
  - Dynamic ARP Inspection (DAI)
  - Configuring ARP
  - Flushing ARP and the Neighbor Table
- Configuring IP Routing
- Static Routing Configuration
  - Configuring Static Routes
  - Example for Configuring IPv4 Static Routes
- VRF Configuration Guide
  - Introduction to VRF
  - Configuration Notes of VRF
  - Configuring a User-defined VRF
  - Enabling Management VRF
  - Example for Configuring Basic VRF
- DHCP Configuration
  - Introduction to DHCP
  - Configuration Notes of DHCP
  - Configuring DHCP Server (IPv4)
  - Configuring DHCP Relay
    - Configuring DHCP Relay (IPv4)
    - Example for Configuring DHCPv6 Relay
    - Example for Configuring DHCP Relay over GRE Tunnel
  - Configuring DHCP Snooping
    - Configuring DHCP Snooping (IPv4)
    - Configuring DHCPv6 Snooping (IPv6)
  - Typical Configuration Example for DHCP Relay and DHCP Snooping
  - DHCPv6 Guard Configuration
    - Overview of DHCPv6 Guard
    - Configuring DHCPv6 Guard
    - Example for Configuring DHCPv6 Guard
  - RFC Lists
- Default Administrative Distance Values
- OSPF (Open Shortest Path First)
  - OSPF Overview
  - Basic OSPF Configuration Tasks
  - Configuring OSPF Route Summarization
  - Basic OSPF Configuration Example
  - OSPF Area Type Configuration Example: NSSA, Stub and Standard Areas
  - OSPF Stub and NSSA Areas with no-summary
  - OSPF Area Range Configuration Guide
  - OSPF Route Redistribution and Route Maps
  - Example for Configuring OSPF with Different VRFs
  - OSPFv3 Configuration Guide
  - OSPF Multi-Instance Support
  - OSPF GR
- ECMP (Equal-Cost Multipath Routing) Configuration
- Symmetric Hash for ECMP Configuration Example
- VRRP Configuration
  - Principle of VRRP
  - Configuration Notes of VRRP
  - Configuring Standard VRRP
  - Configuring Active-Active VRRP
  - VRRP Configuration Example
    - Example for Configuring Standard VRRPv3 for IPv4
    - Example for Configuring Active-Active VRRPv3 for IPv4
    - Example for Configuring Active-Active VRRPv3 for IPv6
- IPv4/IPv6 BGP Configuration
  - BGP Introduction
  - BGP Regular Expressions
  - Basic BGP Configuration
  - Configuring BGP Security
  - Configuring a BGP Route Reflector
  - Configuring BGP Timers
  - Configuring BGP Route Aggregation

        - Configuring BGP Dynamic Neighbors
        - Configuring eBGP Multihop
        - Configuring Removing and Replacing Private ASNs from the AS Path
        - Configuring BGP Multipath
        - Configuring ebgp-requires-policy
        - Enable BGP Read-only Mode
        - Configuring Route Maps for Route Updates
        - BGP Unnumbered
            - Overview of BGP Unnumbered
            - Example for Configuring Basic BGP Unnumbered
            - Example for Configuring BGP Unnumbered EVPN Fabric
        - Configuring BGP Attribute
            - Configuring the AS_Path Attribute
            - Configuring the BGP Community Attribute
            - Configuring the MED Attribute
            - Configuring the Next_Hop Attribute
        - Configuration Examples
            - Example for Configuring Basic BGP Functions
            - Example for Configuring a BGP Route Reflector
            - Example for Configuring BGP Load Balancing
- Routing Map Configuration
    - Routing Map Introduction
    - Configuring Filters
        - Configuring a Community Filter
        - Configuring a Large Community Filter
        - Configuring an AS_Path Filter
        - Configuring an Extended Community Filter
        - Configuring an IP Prefix List
    - Configuring a Routing Map
    - Example for Filtering the Routes to Be Advertised and Receiving
- IPv6 Support
    - IPv6 Neighbor Discovery Configuration
    - PICOS L2/L3 Support for IPv6
    - Enable Path MTU Discovery
- IPv6 Neighbor Discovery Inspection
    - Overview of ND Inspection
    - Configuring ND Inspection
    - Example for ND Inspection
- IPv6 Neighbor Discovery Snooping
    - Overview of ND Snooping
    - Operation Mechanism of ND Snooping
    - Configuring ND Snooping
    - Example for ND Snooping
- VRF Route Leaking Configuration
    - BGP Route Leaking Configuration Example
    - Static Route Leaking Example
- Bidirectional Forwarding Detection (BFD)
    - Introduction of BFD
    - Configuring BFD
        - Configuring Static BFD
        - Configuring Dynamic BFD
    - Configuration Examples of BFD
        - Example for Configuring Single-Hop BFD
        - Example for Configuring Multi-Hop BFD
        - Example for Configuring BFD for BGP
        - Example for Configuring BFD for OSPF
        - Example for Configuring BFD for PIM-SM
    - RFC Lists for BFD
- RIP/RIPng Configuration
    - RIP/RIPng Overview
    - Enabling RIP/RIPng
    - Configuring RIP Version
    - Configuring RIP Route Redistribute
    - Configuring RIPv2 Authentication
    - Configuring RIP to Advertise Default Routes
    - Example for Configuring Basic RIP
    - Example for Configuring Basic RIPng
    - RFC Lists for RIP/RIPng
- Policy-Based Routing (PBR)
    - Overview of PBR
    - Configuring Policy-Based Routing
    - Example for Configuring Policy-Based Routing
- IPv4 Source Guard (IPSG for IPv4)

- IPv6 Source Guard (IPSG for IPv6)
- IPv6 RA Guard Configuration
- IS-IS Configuration
  - IS-IS Overview
  - Configuring IS-IS Basic Function
  - Configuring IS-IS Authentication
  - Configuring LSP Packet Attributes
  - Customizing Routes for IS-IS
  - Configuring IS-IS Timers
    - Configuring the Interval for Sending Hello Messages
    - Configuring the Hello-Multiplier for the Neighbor Holding Time
    - Configuring the Interval for Sending CSNP Messages
    - Configuring the Interval for Sending PSNP Messages
  - Controlling IS-IS Routing Information Exchange
    - Configuring IS-IS Advertising Default Routes
    - Configuring IS-IS Introducing External Routes
  - Adjusting SPF Calculation Time
  - Configuration Examples of IS-IS
    - Basic IS-IS Configuration Example
    - Configuration Example of Interaction Between IS-IS and BGP

ARP Configuration

- Configuring ARP
- Dynamic ARP Inspection (DAI)
- Flushing ARP and the Neighbor Table

Configuring ARP

> **NOTE:**
> A chassis switch supports a maximum of 12000 ARP entries in the ARP table, including both IPv4 ARP entries and IPv6 neighbor entries. Both of which are saved in the same system resource on the switch. One IPv6 neighbor entry takes up two ARP entries.

Configuring ARP Aging Time

In the default setting, the ARP aging time is 1200 seconds.

```
admin@XorPlus# set protocols arp aging-time 600
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a Static ARP Entry

PicOS supports configuring static ARP on VLAN interface, routed interface or sub-interface. The following example shows how to configure a static ARP entry on the VLAN interface.

Step1 Configure a VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 192.168.1.1 prefix-length 24
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Step2 Configure a static MAC entry to create a hardware forwarding entry, where the **interface** is the outbound physical interface.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 static-ethernet-switching mac-address 22:22:22:22:22:22 vlar
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Step3 Configure a static ARP entry.

```
admin@XorPlus#set protocols arp interface vlan-2 address 192.168.1.1 mac-address 22:22:22:22:22:22
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
```

Dynamic ARP Inspection (DAI)

- Introduction
  - Trust Port
  - ARP Packets Validity Checking
  - User Legitimacy Checking
- Configuring Dynamic ARP Inspection
  - Procedure
  - Example for Configuring Dynamic ARP Inspection
    - Networking Requirements
    - Procedure
- Configuring ARP Inspection Access List
  - Procedure
  - Example for Configuring Static ARP Inspection

Introduction

The ARP Inspection feature is used to defend against man-in-the-middle attack scenarios, preventing ARP table entries to be maliciously modified by a forged ARP message sent by an attacker.

Trust Port

ARP inspection divides interfaces into ARP trusted and untrusted ports. On trusted ports, the system does not perform ARP inspection on incoming ARP messages, allowing the ARP messages to pass. However, ARP inspection is required for ARP messages received on the untrusted port interface.

By default, all the interfaces are untrusted ports. You can use the command **set protocols arp inspection trust-port** *<port-name>* to configure an interface as trusted port and use **run show arp inspection interface** to show the trust state of all the interfaces for ARP inspection.

ARP Inspection contains two functions: ARP message validity checking and user legitimacy checking.

ARP Packets Validity Checking

For ARP trusted ports, packets validity checking is not performed; for ARP untrusted ports, the system checks the validity of MAC address and IP address in the ARP packets:

- Check that if the source MAC address in the ARP message and the source MAC address in the Ethernet header are consistent. If so, pass, otherwise discard.
- Check if the source MAC address in the ARP message is all 0 or all 1. All 0 and all 1 source MAC addresses are invalid and the message will be discarded.
- Check if the source IP in the ARP message is all 0, all 1, or the multicast IP address, these IP addresses are invalid and the message will be discarded.

User Legitimacy Checking

For ARP trusted ports, user legitimacy checking is not performed; for ARP untrusted ports, a user legitimacy checking is performed to prevent attacks from spoofing users.

ARP inspection user legitimacy checking is to check the validity of ARP message which supports two of the following implementation and application modes:

1. Dynamic ARP inspection based on DHCP snooping binding table. DHCP snooping is required in this scenario.

However, if ARP inspection is enabled in the VLAN with DHCP relay enabled, DHCP snooping is also required in this same VLAN for ARP inspection to work properly. The system uses the DHCP snooping table to generate ARP entries for ARP inspection.

You can run the command **run show ARP inspection dhcp-binding** to view the ARP entries generated from the DHCP snooping and DHCP relay table.

2. ARP access lists for non-DHCP environments which needs the administrator to configure by CLI commands.

When the switch receives an ARP message, it compares the source IP address and source MAC address of the ARP message with the entries in the ARP access lists (if configured) and the DHCP binding table:

- If the message matches, the user who sent the ARP message is considered as a legitimate user and allows the ARP message to pass.
- Otherwise, it is considered as an attack and the ARP message is discarded.

run show arp inspection statistics vlan command displays the statistics of ARP inspection, such as, discarded and permitted ARP packets.

NOTE:

- If both ARP access lists and dynamic ARP inspection are enabled, the system checks ARP access lists first, if there is no match then the system checks DHCP binding table.
- When ARP inspection is enabled on MLAG peers, we recommend that you don't enable ARP inspection in the peer-link VLAN which is dedicated to transmitting MLAG control plane messages.

However, if ARP inspection is enabled in peer link VLAN, an ARP access list must be configured by the following commands for ARP inspection to make MLAG work normally,

set protocols arp inspection access-list *<acl-name>* **ip** *<ipv4-addr>* **mac-address** *<mac-addr>*

set protocols arp inspection vlan *<peer-vlan-id>* **access-list** *<acl-name>*

where IP, MAC address and VLAN should be configured as the corresponding values of peer link port on the MLAG peer device.

Configuring Dynamic ARP Inspection

Dynamic ARP Inspection checks ARP messages based on DHCP binding table. Therefore, you need to enable the DHCP snooping function for this feature to work properly.

Procedure

Step1 Enable ARP inspection in a VLAN.

set protocols arp inspection vlan <*vlan-id*> **disable** <**true | false**>

Step2 Enable DHCP snooping.

a) Enable DHCP snooping in a VLAN.

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

b) Configure the interface connected to the DHCP server as DHCP snooping trusted interface.

set protocols dhcp snooping trust-port <*interface-name*>

Step3 (Optional) Configure an interface as a trust port on which ARP inspection will not be implemented.

set protocols arp inspection trust-port <*port-name*>

Step4 Commit the configurations.

commit

Example for Configuring Dynamic ARP Inspection

Networking Requirements

- On Pica8 Switch, the interfaces ge-1/1/1 and ge-1/1/2 are in VLAN 2.
- Enable DHCP snooping on VLAN 2.
- Configure the interface connected to the DHCP server (ge-1/1/2) as the DHCP snooping trust interface.
- To prevent man-in-the-middle attacks and prevent the ARP table entries of legitimate users on the device being maliciously modified, enable ARP inspection in VLAN 2.

Figure 1 Dynamic ARP Inspection Network

Procedure

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
```

Step2 Enable ARP inspection in VLAN 2.

```
admin@Xorplus# set protocols arp inspection vlan 2 disable false
```

Step3 Enable DHCP snooping.

```
admin@XorPlus# set protocols dhcp snooping vlan 2 disable false
admin@XorPlus# set protocols dhcp snooping trust-port ge-1/1/2
```

Step4 Commit the configurations.

```
admin@XorPlus# commit
```

Step5 Verify the configurations.

- Run the command **run show arp inspection vlan** <*vlan-id*> to display ARP inspection configured information of a VLAN.

```
admin@Xorplus# run show arp inspection vlan 2
Vlan  Configuration      Static ACL
----   -------------     ----------
2     Enabled            -
```

- Run the**run show arp inspection dhcp-binding** command to view the ARP inspection table. This table includes the ARP entries generated from the DHCP snooping or DHCP relay table.

```
admin@Xorplus# run show arp inspection dhcp-binding
Vlan  IP Address        Mac Address
----  ---------------  -----------------
 2    100.1.1.1         14:18:77:18:2c:b9
```

Configuring ARP Inspection Access List

ARP inspection supports to statically configure ARP access lists through CLI commands in non-DHCP environments, so it does not require to enable DHCP snooping.

NOTE:

When configuring the ARP access list for ARP Inspection, the same IP-MAC cannot exist in multiple access lists.

Procedure

Step1 Enable ARP **inspection** in a VLAN.

set protocols arp inspection vlan <*vlan-id*> **disable** <**true | false**>

Step2 Configure ARP access list for ARP inspection.

set protocols arp inspection access-list <*acl-name*> **ip** <*ipv4-addr*> **mac-address** <*mac-addr*>

Step3 Apply the ARP inspection access list to a VLAN.

set protocols arp inspection vlan <*vlan-id*> **access-list** <*acl-name*>

Step4 (Optional) Configure an interface as a trust port on which ARP inspection will not be implemented.

set protocols arp inspection trust-port <*port-name*>

Step5 Commit the configurations.

commit

Example for Configuring Static ARP Inspection

Configuring ARP access lists is an effective defense against man-in-the-middle attacks and preventing ARP table entries of legitimate users on the device being maliciously modified.

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100
```

Step2 Enable ARP inspection in VLAN 100.

```
admin@Xorplus# set protocols arp inspection vlan 100 disable false
```

Step3 Configure ARP inspection static access list.

```
admin@Xorplus# set protocols arp inspection access-list test1 ip 10.0.0.1 mac-address 00:B0:BC:00:00:00
```

Step4 Apply the ARP inspection access list to a VLAN.

```
admin@Xorplus# set protocols arp inspection vlan 100 access-list test1
```

Note that:

Configure the access-list first and then apply to a VLAN, otherwise it will prompt access-list does not exist when committing this command.

Step5 Commit the configurations.

```
admin@XorPlus# commit
```

Step6 Verify the configurations.

- Run the command **run show arp inspection vlan** <*vlan-id*> to display ARP inspection configured information of a VLAN.

```
admin@Xorplus# run show arp inspection vlan 100
Vlan  Configuration      Static ACL
----   -------------     ----------
100     Enabled          test1
```

- Run command **run show arp inspection vlan** <*vlan-id*> **access-list** <*acl-name*> to display the information for ARP inspection static access list.

```
admin@Xorplus# run show arp inspection access-list test1
Static ACL  IP Address       Mac Address
----------  ---------------  -----------------
Test1       10.0.0.1         00:B0:BC:00:00:00
Static ACL  Applied Vlans
----------  -------------------
Test1       100
```

Flushing ARP and the Neighbor Table

You can manually flush the ARP entry and the IPv6 neighbor table.

Flushing the ARP Entry

```
admin@XorPlus> flush arp all
admin@XorPlus> flush arp ip-address 192.168.1.1
```

Configuring IP Routing

NOTE:

- Layer 3 packets cannot be forwarded normally if IP routing function is disabled.
- Enable IP routing function before using VXLAN.
- IP routing affects only Layer 3 data forwarding, but takes no effect on non-Layer 3 data forwarding of the interface. Therefore, inband management (such as login via SSH) has nothing to do with whether IP routing is enabled or not.
- If the following commit failed message appears when you enable IP routing, the Enterprise License is not installed, and you need to purchase and install the Enterprise License before the L3 feature can be used properly.

```
admin@Xorplus# set ip routing enable true
admin@Xorplus# commit
Command failed: L3 feature is not covered by the installed license key.
Commit failed.
```

To allow users to communicate with users in different VLANs through Layer 3 routing, in addition to configuring Layer 3 interfaces for VLANs, you also need to enable IP routing function on Layer 3 switches.

By default, IP routing function is disabled. If you want to implement the Layer 3 inter-VLAN routing function of the switch, you need to enable the IP routing function first. Similarly, you can configure the system to disable IP routing if you want to disable the Layer 3 inter-VLAN routing function on the switch. When the IP routing function is disabled, the switch can function only as a Layer 2 switch.

Configuring IP Routing

Procedure

- Use the following command to enable or disable IP routing function.

  set ip routing enable [**true | false**]

  The default setting is **set ip routing enable false**. The command takes effect immediately after committing.

Configuration Example

Network Requirement

As shown in Figure 1, User1 and User2 are in the same department of the company but belong to different VLANs and are located on different network segments. Follow the configuration steps below to achieve User1 and User2 can communicate with each other.
1. Create a VLAN and specify the VLAN to which the user belongs.
2. Add an interface to the VLAN.
3. Create a Layer 3 interface and configure the IP address.
4. Enable IP routing function to achieve inter-VLAN routing.

NOTE:

On User1 and User2, add a route with the default gateway to be the IP address of the corresponding Layer 3 VLAN interface.

Figure 1. Network of Inter-VLAN Routing



Procedure

Step1 Create VLAN2 and VLAN3 on Switch.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
```

Step2 Add interfaces connected to user terminals to different VLANs.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 3
```

Step3 Associate a Layer 3 interface with the VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
```

Step4 Configure IP address of the Layer 3 interface.

```
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 192.168.2.2 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 192.168.3.2 prefix-length 24
```

Step5 Enable IP routing function.

```
admin@XorPlus# set ip routing enable true
```

Step6 Commit the Configuration.

```
admin@XorPlus# commit
```

Step7 Verify the Configuration.

- After the configuration is complete, User1 in VLAN2 and User2 in VLAN3 can communicate with each other.
- When IP routing function is disabled on the Switch, User1 in VLAN2 and User2 in VLAN3 will be unreachable when pinging each other.
- Use **show route forward-route brief** command to view the information of IP routing table. If IP routing function is disabled, the command results "**Ip routing is disable**".

```
admin@Xorplus# run show route forward-route brief
Ip routing is disable
```

Static Routing Configuration

This chapter describes the functions, purposes, and applications of static routes, and explains how they can be configured.

- Configuring Static Routes
- Example for Configuring IPv4 Static Routes

Configuring Static Routes

NOTE:

- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.
- The static route that specifies the next hop address and the one that specifies the outgoing interface are not considered for ECMP load sharing, even if they have equal cost.
- If you are configuring a default route in the default VRF, you need to enable management VRF (After enabled by using command set system management-vrf enable true, eth0 will automatically be moved to management VRF from default VRF) to ensure the normal access to eth0 management port.

In L2/L3, all routing entries will be configured to the ASIC switching chip if the outgoing interface is link-up, and the outgoing physical port is learning. The outgoing interface is an L3 interface which can be VLAN interface, routed interface, loopback interface or sub-interface.

Traffic that can be routed will have a route entry in the RIB and the ARP of the next hop; the outgoing interface should be link-up. The traffic will then be soft-routed (i.e., routed by the switch's CPU).

When the switch learns the MAC address of the next-hop, the switch will forward the traffic with the ASIC chip.

Configure static route:

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 192.168.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 192.168.2.1 prefix-length 24
admin@Xorplus# set ip routing enable true
admin@XorPlus# set protocols static route 10.10.1.0/24 next-hop 192.168.2.5
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 10.10.1.0/24 [1/0] via 192.168.2.1, vlan-3, weight 1, 00:40:35


admin@XorPlus# set interface gigabit-ethernet te-1/1/5 routed-interface enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/5 routed-interface name rif-2
admin@XorPlus# set vlans reserved-vlan 800-900
admin@XorPlus# set l3-interface routed-interface rif-2 address 120.2.1.49 prefix-length 24
admin@XorPlus# set protocols static route 8.1.1.0/24 next-hop 120.1.1.45
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, A - Babel, F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 10.10.1.0/24 [1/0] via 192.168.2.1, vlan-3, weight 1, 03:40:35
S>* 8.1.1.0/24 [1/0] via 120.1.1.49, rif-2, weight 1, 01:18:48
```

With the **show route forward-route ipv4 all** command, all the IPv4 route entries in the ASIC chip will be displayed.

```
admin@Xorplus# run show route forward-route ipv4 all
Destination          NextHopMac          Port
---------------      -----------------   ---------
10.10.1.0/24        3C:2C:30:84:E0:81   connected
8.1.1.0/24          3C:2C:30:84:E0:81   te-1/1/5
Total route count:2
```

Example for Configuring IPv4 Static Routes

Unicast routing involves sending data from a single sender to a single receiver, making it a point-to-point routing protocol. Examples of unicast protocols include TCP and HTTP. Various forms of Layer 3 routing are considered unicast, including static routing. Static routing is used to manually configure a routing entry rather than rely on dynamic routing. As the name implies, static routes are fixed routes that do not change. They may be used as a backup to dynamic routing, to ensure a valid path exists between two points.

This document describes an example of how to configure a static route between two hosts in a network using open white box switches running the Pica8 PICOS network operating system.

- Configuration Example
  - Configuring Switch A
  - Configuring Switch B
  - Configuring Switch C

Configuration Example

An example of configuration with static routing is shown in Fig. 5-1. Host A and Host B should be able to communicate with each other. Host A and Host B should be able to communicate with the gateway (e.g., access Internet).

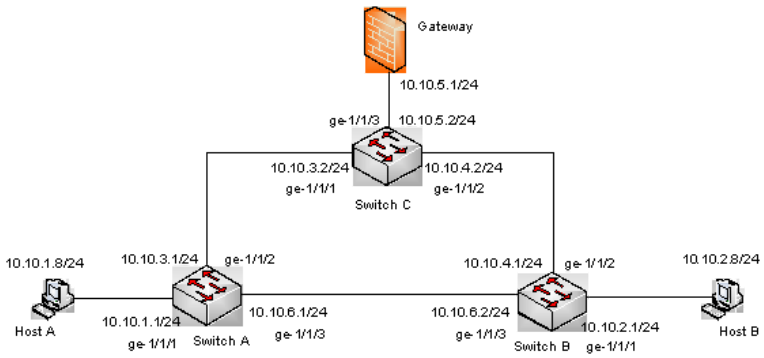


Figure 5-1. Static routing configuration.

Configuring Switch A

For Switch A, configure 3 VLAN interfaces for networks 10.10.1.1/24, 10.10.3.1/24, and 10.10.6.1/24. Also configure a static route to 10.10.2.0/24 and a default route.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set vlans vlan-id 4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 4
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set vlans vlan-id 4 l3-interface vlan-4
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.3.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-4 address 10.10.6.1 prefix-length 24
admin@XorPlus# set ip routing enable true
admin@XorPlus# set protocols static route 10.10.2.0/24 next-hop 10.10.6.2
admin@XorPlus# set protocols static route 0.0.0.0/0 next-hop 10.10.3.2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Verify the static route entry in the RIB as follows:

```
admin@XorPlus# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 10.10.2.0/24 [1/0] via 10.10.6.1, vlan-4, weight 1, 00:40:35
S>* 0.0.0.0/0 [1/0] via 10.10.3.1, vlan-3, weight 1, 05:00:04
```

Configuring Switch B

Configure 3 VLAN interfaces for networks 10.10.2.1/24, 10.10.4.1/24, and 10.10.6.2/24. Then, configure a static route to 10.10.1.0/24 and a default route.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set vlans vlan-id 4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 4
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set vlans vlan-id 4 l3-interface vlan-4
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.2.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.4.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-4 address 10.10.6.2 prefix-length 24
admin@XorPlus# set ip routing enable true
admin@XorPlus# set protocols static route 10.10.1.0/24 next-hop 10.10.6.1
admin@XorPlus# set protocols static route 0.0.0.0/0 next-hop 10.10.4.2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Verify the static route entry in the RIB:

```
admin@XorPlus# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 10.10.1.0/24 [1/0] via 10.10.6.1, vlan-4, weight 1, 00:40:35
S>* 0.0.0.0/0 [1/0] via 10.10.4.1, vlan-3, weight 1, 05:00:04
```

Configuring Switch C

Configure 3 VLAN interfaces for networks 10.10.3.2/24, 10.10.4.2/24, and 10.10.5.2/24. Then, configure a static route to 10.10.1.0/24 and a default route.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set vlans vlan-id 4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 4
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set vlans vlan-id 4 l3-interface vlan-4
admin@XorPlus# commit
Commit OK.
```

```
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.3.2 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.4.2 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-4 address 10.10.5.2 prefix-length 24
admin@XorPlus# set ip routing enable true
admin@XorPlus# set protocols static route 10.10.1.0/24 next-hop 10.10.3.1
admin@XorPlus# set protocols static route 10.10.2.0/24 next-hop 10.10.4.1
admin@XorPlus# set protocols static route 10.10.6.0/24 next-hop 10.10.3.1
admin@XorPlus# set protocols static route 0.0.0.0/0 next-hop 10.10.5.1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Verify the static route entry in the RIB:

```
admin@XorPlus# run show route static
RIB entry for static
====================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 10.10.1.0/24 [1/0] via 10.10.3.2, vlan-2, weight 1, 00:40:35
S>* 10.10.2.0/24 [1/0] via 10.10.4.2, vlan-3, weight 1, 00:40:35
S>* 10.10.6.0/24 [1/0] via 10.10.3.2, vlan-2, weight 1, 00:40:35
S>* 0.0.0.0/0 [1/0] via 10.10.5.2, vlan-4, weight 1, 05:00:04
```

VRF Configuration Guide

- Introduction to VRF
- Configuration Notes of VRF
- Configuring a User-defined VRF
- Enabling Management VRF
- Example for Configuring Basic VRF

Introduction to VRF

NOTE:

PICOS supports only VRF-Lite, a lighter version of VRF, referring to VRF without MPLS.

- VRF Characteristics
- Application Scenarios
- Default VRF
  - In-band Management Interface
- Management VRF
- Management Services
- User-defined VRF

VRF (Virtual Routing and Forwarding) is a technology that virtualizes a single physical routing device into multiple virtual routing devices, each of them being (relatively) independent of each other, allowing for overlapping subnets, separate routing tables to make Layer 3 segregated, separate ARP tables and separate sets of Layer 3 interfaces assigned to each VRF.

Figure 1 Multiple VRF Process Modules on One Pica8 Switch

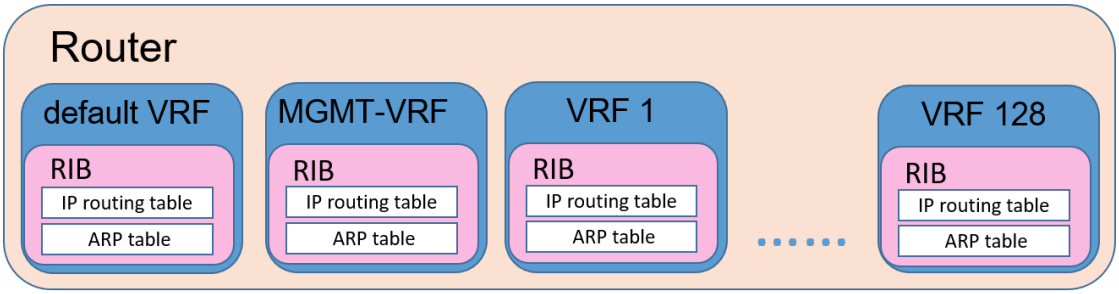


Figure 1 shows multiple VRF process modules on one Pica8 switch. Pica8 switches support multiple VRF instances: one default VRF, one management VRF and multiple user-defined VRFs. IP routing and traffic is separated between the VRFs. By default, PICOS starts up with only default VRF, which cannot be deleted. User can create other VRFs based on the requirements for route separation. The command **set system management-vrf enable** <true | false> can be used to enable management VRF and **set ip vrf** <*vrf-name*> [**description** <*string*>] can be used to create the user-defined VRFs. A maximum of 128 user-defined VRFs can be created on a Pica8 switch.

Currently, default VRF and user-defined VRFs support static routing and other routing protocols (BGP, OSPF, RIP, PIM). However, Management VRF does not support any routing protocols, including static routing.

The following sections describe the VRF characteristics and application scenarios, then details how to use default VRF, management VRF and user-defined VRFs.

VRF Characteristics

- Each VRF has an independent routing table and ARP table to implement independent routing and forwarding functions.
- Each VRF has an independent address space. This allows address overlapping between different VRFs without address conflicts occurring on the same device.
- Users in the same VRF can communicate with each other, but users in different VRFs cannot communicate with each other.
- As with the introduction of management VRF, Out of Band (OOB) management flow is completely separate from data flow, which enhances the security of the management network.

Application Scenarios

This document lists several use cases which can be deployed with VRFs as follows,

- User can deploy VRF function to solve the problem of insufficient IP addresses, as different VRFs have different address spaces which allows address overlapping between different VRFs.
- User can deploy VRF function to achieve traffic isolation of different users and increase data communication security, as the communication between different tenants is segregated in different VRFs.
- User can enable management VRF to separate the Out of Band management traffic from the data traffic, thus to enhance the security of the management network.
- VRF virtualizes a single physical routing device into multiple virtual routing devices; this can save hardware costs.

Default VRF

By default, all the L3 interfaces (VLAN interface, loopback interface, routed interface or sub-interface) and Ethernet0 management interface, and their IP route tables share one VRF - the default VRF. When a L3 interface is created, it is in the default VRF if not explicitly bound to any VRF. However, user can bind an existing Layer 3 interface to a user-defined VRF.

Ethernet0 is used for Out of Band (OOB) management, the L3 interfaces can be used for in-band (IB) management or transmission of data traffic.

Default VRF supports static routing and other routing protocols (BGP, OSPF, RIP, PIM).

In-band Management Interface

By default, the user cannot remotely log in and manage the switch through an L3 interface. PICOS provides in-band management in default VRF. In-band management provides a method of access to the switch even if the Ethernet0 interface is down. You can enable in-band management function to perform the SSH, TELNET, SNMP and HTTP services through any one of the L3 interfaces in the default VRF.

For example,

Set VLAN interface VLAN400 in the default VRF as the in-band management port.

```
admin@Xorplus# set system inband vlan-interface VLAN400
admin@Xorplus# commit
```

In-band management provides a method of access to the switch even if the Ethernet0/1 interface is down.

NOTE:

- Only the L3 interface in the default VRF can be set as the in-band management port. If a L3 interface has been set as an in-band management port, it cannot be bound to other VRFs.
- A maximum of four L3 VLAN interfaces in the default VRF can be set as the in-band management ports by using **set system inband vlan-interface**<*vlan-interface*> command.
- By default, all the management services (including **802.1X / OVSDB management protocol / SNMP trap / sFlow / syslog / NTP / TACACS+/RADIUS**) run in default VRF. If management VRF is enabled, you have to consider which VRF (default VRF or management VRF) will be used to run management services, see the **Management Services** for details.

Management VRF

By default, PICOS starts up with only default VRF, management VRF function is disabled. To enhance the security of the management network, and prevent attacks by illegal users, users can use command **set system management-vrf enable** true to enable management VRF.

Once management VRF is enabled, a VRF with fixed name **mgmt-vrf** is created automatically by the system, and the Eth0 management interface is automatically moved from the default VRF to the management VRF. As long as the management VRF is not disabled, Eth0 is always in the management VRF. Eth0 will return from the management VRF to the default VRF only when management VRF is disabled by setting **set system management-vrf enable** false.

Management VRF is dedicated to transmit the OOB management traffic. Other VRFs are used to transmit the data traffic, thus separating the OOB management traffic from the data traffic effectively.

The management services (including **802.1X / OVSDB management protocol / SNMP trap / sFlow / syslog / NTP / TACACS+/RADIUS**) are running in default VRF by default. However, when management VRF is enabled and Eth0 is used for management services, the management services need to be manually moved from the default VRF into the management VRF by using relevant CLI commands.

For example, if you want to enable management VRF and use the Eth0 management interface for NTP service, the VRF-related configurations are as follows. For more details, see **Management Services.**

```
admin@Xorplus# set system management-vrf enable true
admin@Xorplus# set system ntp vrf vrf mgmt-vrf
admin@Xorplus# commit
```

Management VRF configuration notes:

- Only Eth0 management interfaces can run in the management VRF, no other L3 interfaces or loopback interfaces can run in the management VRF.
- Management VRF supports neither static routing nor any other dynamic routing protocol.

Management Services

To properly use management services, the following descriptions in this section provide a guidance.

By default, all the management services (including **802.1X / OVSDB management protocol / SNMP trap / sFlow / syslog / NTP / TACACS+/RADIUS**) run in default VRF. If management VRF is enabled, Eth0 interface is automatically moved from the default VRF to the management VRF, you have to decide which VRF (default VRF or management VRF) will be used to run the management services.

1. syslog/NTP/TACACS+/RADIUS/SNMP Trap/sFlow/NAC/OVSDB

Management services (referring to syslog/NTP/TACACS+/RADIUS/SNMP Trap/sFlow/NAC /OVSDB) are bound to default VRF at system startup. They can move from default VRF to management VRF and vice versa by using the following CLI commands.

set system syslog vrf mgmt-vrf

set system ntp vrf mgmt-vrf

set system aaa radius vrf mgmt-vrf

set system tacacs-plus radius vrf mgmt-vrf

set protocols snmp trap-group vrf mgmt-vrf

set protocols sflow collector *<ip-address>* **vrf mgmt-vrf**

set protocols dot1x aaa vrf mgmt-vrf

set protocols ovsdb controller *<controller-name>* **vrf mgmt-vrf**

These management services cannot be bound to a user-defined VRF.

Whether the management service is in the default VRF or the management VRF, you need to ensure that the server relevant to the management service (e.g. syslog server, TACACS+ server) is route reachable in the VRF running the management service.

For example,

If you want to enable management VRF and use the Eth0 management interface for NTP service, NTP service needs to be manually moved from the default VRF into the management VRF by using CLI command **set system ntp vrf mgmt-vrf**. The VRF-related configurations are as follows:

```
admin@Xorplus# set system management-vrf enable true
```

```
admin@Xorplus# set system ntp vrf mgmt-vrf
admin@Xorplus# commit
```

2. ssh/scp/tftp/ping/traceroute/apt-get

When executing ssh/scp/tftp/ping/traceroute/apt-get commands, the system looks for the next-hop route in default VRF by default. If management VRF is enabled, and Eth0 is used as the route interface, you have to add the VRF parameter in the command to specify that finding the next-hop route in the management VRF.

- At the Linux prompt

If management VRF is enabled, and you want to find the next-hop route in management VRF when running the commands **traceroute/SCP/ping/apt get/SSH** at Linux prompt, that is, using Eth0/1 management interface as the route interface, you have to add **ip vrf exec mgmt-vrf** before the commands.

The example format of these commands is shown below:

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> **traceroute** 10.10.51.11

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> **scp** admin@10.10.51.18:/home/Pica8.pm

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> ping 10.10.51.1

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> apt-get update

sudo ip vrf exec <**mgmt-vrf|***vrf-name*> ssh <*ip-address*>

ip vrf exec <**mgmt-vrf|***vrf-name*> is added to specify which VRF to run the command in. If not specified, find the next hop routing information from the default VRF.

- At PICOS CLI prompt

If management VRF is enabled, and you want to find the next-hop route in management VRF when running the commands ping/traceroute/tftp at PICOS CLI prompt, that is, using Eth0/1 management interface as the route interface, you need to add **vrf mgmt-vrf** before the commands.

ping/traceroute/tftp commands are shown below,

ping <ip-address> [<packets>] [**vrf** <**mgmt-vrf** | *vrf-name*>] [**source** <source-ip-address >] [**deadline** <deadline-time>] [**ttl** <ttl-value>] [**interval** <interval-value>] [**pattern** <pattern-value>] [**size** <size-value>] [**tos** <tos-value>]

traceroute <ipv4-address> [**vrf** <**mgmt-vrf** | *vrf-name*>]

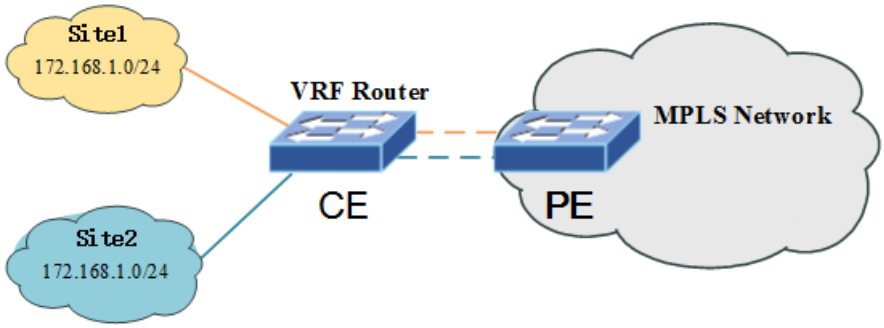
file tftp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*> [**vrf** <**mgmt-vrf** | *vrf-name*>]

[**vrf** <**mgmt-vrf** | *vrf-name*>] is used to specify which VRF to run the command in. If no VRF is specified, find the next hop routing information from the default VRF. For details about the usage of each parameter, see section Command Reference.

User-defined VRF

By default, all the L3 interfaces and their IP route tables are in the default VRF. User can create multiple new VRFs with the VRF definition command **set ip vrf** <*vrf-name*> [**description** <*string*>], and then add the Layer 3 interfaces and their route settings to different VRFs to run services in these VRFs. The system segregates the IP routing table, ARP table, hardware forwarding table, and host hardware forwarding table of different VRFs on one customer edge (CE) device. A maximum of 128 user-defined VRFs can be created.

Figure 2 Networking diagram of VRF



In **Figure 2**, when implementing VRF function on the CE device for different L3 access interfaces, users from Site1 and Site2 can use overlapping IP addresses when accessing the internet through the CE and have segregated users' routing spaces on the CE device.

When the CE switch receives the data packets, it looks up the IP routing table divided by the VRF, which is bound to the ingress Layer 3 interface, and then forwards the data packets based on the routing entry in this VRF.

VRF implements data traffic segregation among different customers while sharing the same physical router device, that is to say, users in the same VRF could communicate with each other, but it could not communicate with each other in different VRFs.

Configuration Notes of VRF

When configuring VRF on a device, pay attention to the following points:

- Enable IP routing function before using VRF function.
- Currently, default VRF supports static routing and other routing protocols (BGP, OSPF, RIP, PIM), the user-defined VRFs support static routing and OSPF routing protocol. However, management VRF supports neither static routing nor any other dynamic routing protocols.
- VRRP supports VRF function by binding the Layer 3 interface to a specified VRF.
- A switch supports a maximum of 128 VRFs.
- A Layer 3 interface can't belong to more than one VRF, but one VRF can be bound to multiple Layer 3 interfaces. This is limited by the maximum number of Layer 3 VLAN interfaces a switch supports. A switch supports a maximum of 255 Layer 3 interfaces.
- Loopback interface can be configured in the default VRF, management VRF or the user-defined VRFs.
- If a VLAN interface changes the configuration to bind to another VRF, the IPv6 addresses of the interface need to be reconfigured to make it valid.
- For AmpCon environment, PICOS will restart the OpenVPN connection between the switch and AmpCon Server, switching the OpenVPN connection to the management VRF, if Eth0 is used to connect to the AmpCon Server and management VRF is enabled. This may cause a short interruption in communication between AmpCon Server and the switch.

Configuring a User-defined VRF

The VRF configuration process is in the following steps:

1. Enable IP routing function before using VRF function.
2. Create a VRF for the tenant.
3. Bind one or more L3 interfaces (VLAN interfaces, loopback interfaces, routed interfaces or sub-interfaces) to the VRF.
4. Configure static routes or OSPF routing protocol into the VRF table.

Procedure

Step1 Enable IP routing function before using VRF function.

set ip routing enable <**true** | **false**>

Step2 Create a VRF for the tenant.

set ip vrf <*vrf-name*> [**description** <*string*>]

Step3 Bind one or more L3 interfaces to the VRF.

- Bind one or more VLAN interfaces to the VRF.

  a) Configure VLAN ID.

  set vlans vlan-id <*vlan-id*>

  b) Configure the interface to a VLAN.

  set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

  c) Configure the IP address of the Layer 3 interface.

  set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

  d) Associate a Layer 3 interface with a VLAN.

  set vlans vlan-id <*vlan-id*> **l3-interface** <*interface-name*>

  e) Bind the Layer 3 VLAN interface to a VRF.

  set l3-interface vlan-interface <*interface-name*> **vrf** <*vrf-name*>

- Bind one or more routed interfaces/sub-interfaces to the VRF.

  a) Enable routed interface.

  set interface gigabit-ethernet <*interface-name*> **routed-interface enable** <**true | false**>

  set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

  b) Configure reserved-vlan for the routed interface.

  set vlans reserved-vlan <*reserved-vlan*>

  c) (Optional) Create the sub-interface and add it into a VLAN.

  set interface aggregate-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

  d) Configure the IP address of the routed interface.

  set l3-interface routed-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix-number*>

  e) Bind the routed interface to a VRF.

  set l3-interface routed-interface <*interface-name*> **vrf** <*vrf-name*>

- Bind one or more loopback interfaces to the VRF.

  a) Create a loopback interface and configures its IP address.

  set l3-interface loopback <*loopback-name*> **address** <*ip-address*> **prefix-length** <*int*>

  b) Bind the loopback interface to a VRF.

  set l3-interface loopback <*interface-name*> **vrf** <*vrf-name*>

Step4 (Optional) Configure a static route entry into the VRF.

set protocols static [**vrf** <*vrf-name*>] **route** <*ip-address*> **next-hop** <*nexthop-address*>

Step5 (Optional) Configure static ARP entries.

set protocols arp interface <*interface-name*> **address** <*ip-address*> **mac-address** <*mac-address*>

The ARP entries are associated with the VRF by binding the Layer 3 VLAN interface to the VRF.

Enabling Management VRF

Procedure

Step1 Enable IP routing function before using VRF function.

set ip routing enable <**true** | **false**>

Step2 Enable management VRF.

set system management-vrf enable <true | false>

Step3 (Optional) Set static IP addresses for management interface eth0.

set system management-ethernet eth0 ip-address {**IPv4** | **IPv6}** <*ip_address*>

> **NOTE:**
> If the static IP address is not assigned, the system will try to dynamically obtain the management port IP address from the DHCP server which is also the factory setting.

Step4 Set the gateway address for management interface eth0.

set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}<*ip_address*>

Step5 Configure to run the management services in the management VRF.

When management VRF is enabled, the management services (including **802.1X / OVSDB management protocol / SNMP trap / sFlow / syslog / NTP / TACACS+/RADIUS**) are still running in default VRF by default. If Eth0 is used for management services, the management services need to be moved into the management VRF manually by using relevant CLI commands.

set system syslog vrf <mgmt-vrf | default>

set system ntp vrf <**mgmt-vrf** | **default>**

set system aaa radius vrf <mgmt-vrf | default>

set system tacacs-plus radius vrf <mgmt-vrf | default>

set protocols snmp trap-group vrf <mgmt-vrf | default>

set protocols sflow collector <*ip-address*> **vrf** <**mgmt-vrf** | **default**>

set protocols dot1x aaa vrf <mgmt-vrf | default>

set protocols ovsdb controller <*controller-name*> **vrf <mgmt-vrf | default>**

Step6 You can use the **run show system management-ethernet eth0** command to view the information of the management interface.

Once management VRF is enabled, a VRF with fixed name **mgmt-vrf** is created automatically by the system, and the Eth0 management interface is automatically moved from the default VRF to the management VRF.

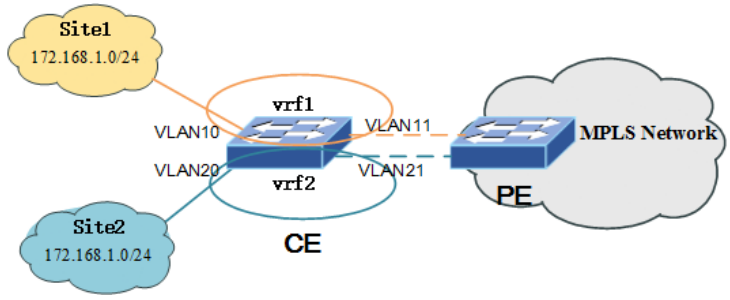
```
admin@Xorplus# run show system management-ethernet
eth0    Hwaddr: e0:07:1b:c9:20:9a   State: UP
    Master: mgmt-vrf
    Gateway  : 10.10.51.1
    Inet addr:
               10.10.51.166/24
               fe80::e207:1bff:fec9:209a/64
    Traffic statistics
    Input Packets.....................4685
    Input Bytes.......................305542
    Output Packets....................109
    Output Bytes......................8566
```

Example for Configuring Basic VRF

- Networking Requirements
- Procedure
- Verify the Configuration

Networking Requirements

Figure 1. VRF Configuration Example



As shown in Figure 1, users of Site1 and Site2 use overlapping IP addresses when accessing the internet from an interface of CE. Deploy VRF function on the CE to segregate the users' routing spaces on Site1 and Site2.

- Configure VRFs vrf1 and vrf2 on CE.
- Create Layer 3 VLAN interfaces VLAN10 and VLAN20 on user access interface te-1/1/3, Layer 3 VLAN interfaces VLAN11 and VLAN21 on the interface te-1/1/4 connected to PE. Set the overlapping IP address 172.168.1.1 to VLAN10 and VLAN20, 192.168.2.1 to VLAN11 and VLAN21.
- Bind the Layer 3 VLAN interfaces VLAN10 and VLAN11 to vrf1, VLAN20 and VLAN21 to vrf2.
- Configure a static route for each VRF for data forwarding. For example, the destination network segment is 10.10.1.0/24, the next hop is 172.168.1.3.

Procedure

Step1 Enable IP routing function before using VRF function.

```
admin@XorPlus# set ip routing enable true
```

Step2 Create two VRFs.

```
admin@Xorplus# set ip vrf vrf1 description East
admin@Xorplus# set ip vrf vrf2 description West
```

Step3 Configure the VLAN and L3 VLAN interface.

```
admin@XorPlus# set vlans vlan-id 10
admin@XorPlus# set vlans vlan-id 20
admin@XorPlus# set vlans vlan-id 11
admin@XorPlus# set vlans vlan-id 21
admin@XorPlus#set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus#set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 10
admin@XorPlus#set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 20
admin@XorPlus#set interface gigabit-ethernet te-1/1/4 family ethernet-switching port-mode trunk
admin@XorPlus#set interface gigabit-ethernet te-1/1/4 family ethernet-switching vlan members 11
admin@XorPlus#set interface gigabit-ethernet te-1/1/4 family ethernet-switching vlan members 21
admin@XorPlus# set l3-interface vlan-interface vlan10 address 172.168.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan20 address 172.168.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan11 address 192.168.2.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan21 address 192.168.2.1 prefix-length 24
admin@XorPlus# set vlans vlan-id 10 l3-interface vlan10
admin@XorPlus# set vlans vlan-id 20 l3-interface vlan20
admin@XorPlus# set vlans vlan-id 11 l3-interface vlan11
admin@XorPlus# set vlans vlan-id 21 l3-interface vlan21
```

Step4 Bind the Layer 3 VLAN interface to the VRF.

```
admin@XorPlus# set l3-interface vlan-interface vlan10 vrf vrf1
admin@XorPlus# set l3-interface vlan-interface vlan11 vrf vrf1
admin@XorPlus# set l3-interface vlan-interface vlan20 vrf vrf2
admin@XorPlus# set l3-interface vlan-interface vlan21 vrf vrf2
```

Step5 (Optional) Configure a static route entry into the VRF, the destination network segment is 10.10 1.0/24, the next hop is 172.168.1.3.

```
admin@XorPlus# set protocols static vrf vrf1 route 10.10.1.0/24 next-hop 172.168.1.3
admin@XorPlus# set protocols static vrf vrf2 route 10.10.1.0/24 next-hop 172.168.1.3
```

Verify the Configuration

- You can use the **run show vrf** command to view the binding information between VRFs and the Layer 3 VLAN interfaces.

```
admin@Xorplus# run show vrf
Vrf          Description       Interfaces
----------   ---------------   --------------------
vrf1                           vlan10,vlan11
vrf2                           vlan20,vlan21
```

- You can use the **run show route vrf** command to check the routing table information of the specific VRF.

```
admin@XorPlus# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

VRF vrf1:
S>* 10.10.1.0/24 [1/0] via 172.168.1.3, vlan10, weight 1, 00:00:45
C>* 172.168.1.0/24 is directly connected, vlan10, 00:04:43
C>* 192.168.2.0/24 is directly connected, vlan11, 00:04:45

admin@XorPlus# run show route vrf vrf2
show ip route vrf vrf2
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

VRF vrf2:
S>* 10.10.1.0/24 [1/0] via 172.168.1.3, vlan20, weight 1, 00:00:59
C>* 172.168.1.0/24 is directly connected, vlan20, 00:04:56
C>* 192.168.2.0/24 is directly connected, vlan21, 00:04:59
```

- You can use the **run show route forward-route** command to check the hardware route forwarding table information of the specific VRF.

```
admin@XorPlus# run show route vrf vrf1 forward-route ipv4 all
Destination          NextHopMac          Port
---------------      -----------------   ---------
192.168.2.0/24       CC:37:AB:BE:0E:D1   connected
172.168.1.0/24       CC:37:AB:BE:0E:D1   connected
10.10.1.0/24         04:7D:7B:62:93:FF   te-1/1/3
```

DHCP Configuration

- Introduction to DHCP
- Configuration Notes of DHCP
- Configuring DHCP Server (IPv4)
- Configuring DHCP Relay
- Configuring DHCP Snooping
- Typical Configuration Example for DHCP Relay and DHCP Snooping
- DHCPv6 Guard Configuration
- RFC Lists

Introduction to DHCP

- Overview
- DHCP Snooping and DHCP Relay Networking Applications
- DHCP Option 82
  - Packet Format
  - How to Handle Option 82?
  - Option 82 trust-all
- Interaction with Other Protocols
  - MLAG
  - VRRP

Overview

Dynamic Host Configuration Protocol (DHCP) dynamically configures and uniformly manages network parameters of the hosts in a TCP/IP network, and allocates IP addresses to the network hosts. PICOS switch supports two basic DHCP functions: DHCP snooping and DHCP relay.

DHCP snooping is a network security feature, which is used to ensure that DHCP clients obtain IP addresses from legitimate DHCP servers, and record the binding relationship between IP addresses and MAC addresses of DHCP clients, so as to prevent DHCP attacks on the network.

Device enabled with DHCP snooping forwards the DHCP request messages from the DHCP client to the legitimate DHCP server through the trust interface, then generates a DHCP snooping binding table according to the DHCP Ack message responded by the DHCP server. The DHCP snooping binding table will be synchronized to ARP inspection table to validate ARP packets in a network to prevent ARP attacks and ARP request message flood, for details about Dynamic ARP Inspection (DAI), please refer to Dynamic ARP Inspection (DAI).

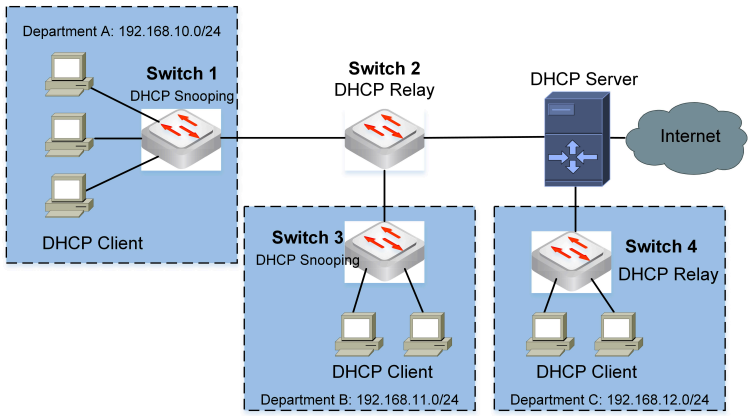
> NOTE:
>
> If Dynamic ARP Inspection (DAI) is to be deployed on the device, when configuring from the CLI, it is required to enable DAI before DHCP snooping can be enabled to make the two features function normally.

DHCP relay is a Layer 3 feature. When the DHCP client and DHCP server are not in the same physical subnet, DHCP relay can be deployed on the Layer 3 device laid between the DHCP client and DHCP server to forward DHCP messages, implementing allocation of IP addresses to the network hosts across different Layer 3 subnets.

DHCP Snooping and DHCP Relay Networking Applications

As shown in figure 1, an enterprise has Department A, Department B and Department C, the gateway server of the enterprise network serves as the DHCP server. The hosts in the three departments are not in the same subnet with the DHCP server. The enterprise wants to dynamically assign IP addresses to the hosts of all the departments by the same DHCP server. The network administrator can deploy a DHCP relay agent between the hosts and the DHCP server to achieve this.

Figure 1 DHCP snooping and DHCP relay networking



Usually, the DHCP relay agent is deployed on the gateway device of the departments, the DHCP server can be deployed on the gateway of the enterprise, or a dedicated DHCP server.

As DHCP request messages are broadcasted in the same subnet, there are often DHCP attacks in the network (e.g., DHCP Server Spoofing, Denial of Service attacks, etc.). In order to prevent attacks by DHCP messages and to improve security, DHCP snooping can be deployed between the DHCP clients and DHCP server to ensure that DHCP clients obtain IP address from the legitimate DHCP server. DHCP snooping is generally deployed on devices close to the DHCP client (e.g., switch 1 and switch 3).

> NOTE:
>
> DHCP snooping and DHCP relay are two modules which are working independently and in parallel. If both DHCP snooping and DHCP relay are enabled on one switch, the DHCP messages will be processed and forwarded by the two modules independently.

DHCP Option 82

Option 82 records the location information of the DHCP client, it can be configured on a DHCP relay or DHCP snooping device. For the DHCP packet received from the DHCP client, the Option 82 carried in that packet will be processed according to the Option 82 policy before sending to the DHCP server.

DHCP server allocates IP addresses and other parameters to the clients based on the Option 82 information carried in the DHCP packet, which provides more flexible address allocation schemes.

Option 82 contains two common sub-options: Circuit ID and Remote ID. Circuit ID is mainly used to identify the VLAN and the interface of the client, Remote ID identifies the device from which the client accessed, usually the MAC address of the device.

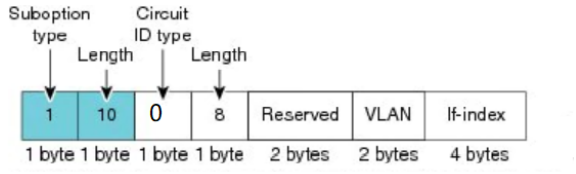
Packet Format

Circuit ID Sub-option

Circuit ID includes three types: Type 0 (value is port index), Type 1 (value is port name + VLAN ID) and Type 2 (value is port description + VLAN ID). The format is listed below by types.

- Type 0 (port index)

Circuit ID type is 0, where physical or LAG interface is used for Circuit ID sub-option.

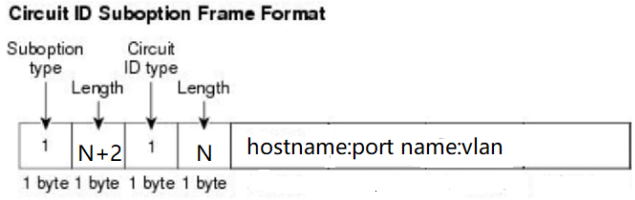


When configuring DHCP snooping and DHCP relay in MLAG topology, MLAG Link ID and Port Index are used for circuit ID field with an offset, see the following table for details:

	MLAG Port	Non-MLAG Port
MLAG Node 0	512 + MLAG Link ID	Local Port Index
MLAG Node 1	512 + MLAG Link ID	1024 + Local Port Index

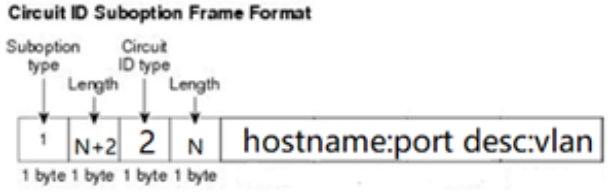
- Type 1 (port name)

Circuit ID type is 1, where port name and VLAN ID make up the Circuit ID sub-option value.



- Type 2 (port description)

Circuit ID type is 1, where port name and VLAN ID make up the Circuit ID sub-option value.

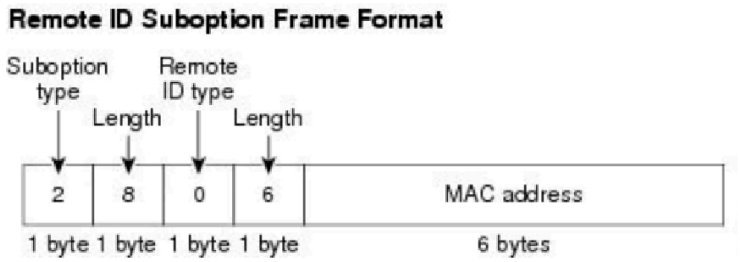


Remote ID Sub-option

Remote ID includes two types: Type 0 (value is system MAC) and Type 1 (value is host name). The format is listed below by types.

- Type 0 (system MAC)

Remote ID type is 0, where system MAC is used for Remote ID sub-option.



Note that: The format of DHCP Option 82 sub-options remote ID is fixed as MLAG domain MAC address in MLAG topology.

- Type 1 (hostname)

Remote ID type is 1, where hostname is used for Remote ID sub-option.

How to Handle Option 82?

The system handles Option 82 in the received DHCP packets according to the following rules:

- When a DHCP Discover/Request/Release/Decline/Inform message **without giaddr** but **with Option 82** is received,
  - If Option 82 trust-all is disabled, then drop the message.
  - If Option 82 trust-all is enabled, such kind of message is processed according to the user configuration of Option 82 policy. There are four types of operations that can be set for Option 82 policy: **Keep**, **Drop**, **Insert** and **Replace**. The default operation is **Keep** which means Option 82 in the DHCP message received from the DHCP client remains unchanged and forwarded.
- When a DHCP Discover/Request/Release/Decline/Inform message of any other type but the one above, the message is allowed on receiving and processed depending on the Option 82 policy.
- When a DHCP Offer/Ack/Nak message **without Option 82** is received, the message is forwarded without Option 82.
- When a DHCP Offer/Ack/Nak message **with Option 82** is received, Option 82 is removed before the message is forwarded.

Option 82 settings are supported respectively on both DHCP relay agent or on the Layer 2 access device enabled with DHCP snooping function. The related commands are listed below:

Set Option policy for DHCP snooping:

set protocols dhcp snooping vlan <*vlan-id*> **option82-policy** <**drop | keep | insert | replace**>

When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of sub-options circuit ID and remote ID:

set protocols dhcp snooping option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp snooping option82 remote-id <system-mac | hostname>

Set Option policy for DHCP Relay:

set protocols dhcp relay interface <*vlan-interface-name*> **option82-policy** <**drop | keep | insert | replace**>

When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of sub-options circuit ID and remote ID:

set protocols dhcp relay option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp relay option82 remote-id <system-mac | hostname>

We can use the following table to summarize the Option 82 policy.

Received Packet / Option82 Policy	No Option82	Only Circle ID	Only Remote ID	Circle ID + Remote ID
drop	The packet is forwarded without changing option 82.	The packet is dropped.	The packet is dropped.	The packet is dropped.
keep	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.
insert	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: unchanged. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: unchanged.	The packet is forwarded. Circle ID: unchanged. Remote ID: unchanged.
replace	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: replaced with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: replaced with the value configured.

NOTE:

DHCP snooping and DHCP relay can handle Option 82 independently and in parallel since they are two completely separated modules.

Option 82 trust-all

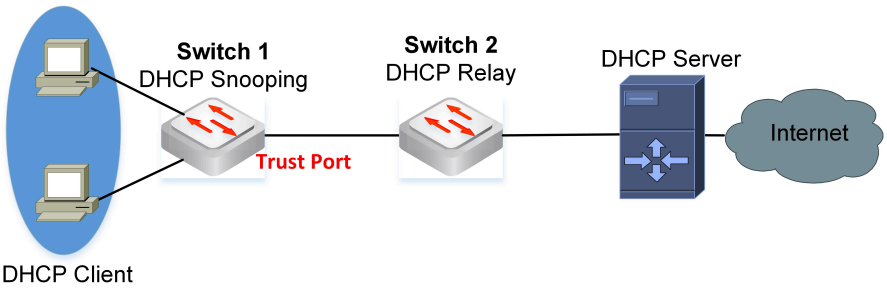
DHCP Discover/Request/Release/Decline/Inform packets received on the switch without giaddr but containing Option 82 are dropped by default. However, if Option 82 trust all function is enabled, such packets will be allowed and processed.

Therefore, when configuring the Option 82 policy, you need to take into consideration the network topology and the configuration of trust all together, especially if there is a switch between the client and the relay agent/the DHCP snooping enabled device that may insert Option 82. Enable DHCP Option 82 trust all on this device to ensure that these packets do not get dropped.

For example, in the following topology, the configurations on Switch 1 and Switch 2 are:

- DHCP snooping is enabled on Switch 1, and DHCP relay is enabled on Switch 2.
- DHCP snooping trust port is configured on the physical or L2 aggregated port towards Switch 2 on Switch 1.

Figure 2 DHCP Snooping and DHCP Relay Topology



DHCP snooping Option 82 can be enabled on Switch 1, and DHCP relay Option 82 can be enabled on Switch 2. It is optional. But if Option 82 is inserted on Switch 1, DHCP relay Option 82 trust all should be enabled on Switch 2.

Interaction with Other Protocols

MLAG

Devices in the MLAG topology support enabling DHCP snooping or DHCP relay function on the MLAG peer devices to implement address allocation for the DHCP clients.

When configuring DHCP snooping and DHCP relay in MLAG topology, pay attention to the following points:

- DHCP snooping configurations, such as Option 82 policy, VLANs enabled or disabled DHCP snooping, should be configured identically on both MLAG peer devices, the inconsistent configuration can cause undesirable behavior in the traffic flow.
- If the VLANs enabled or disabled DHCP snooping are not identical on MLAG peer devices or the MLAG global configuration are not identical on MLAG peer devices, the DHCP binding table entries will be cleared.
- When configuring DHCP snooping, the ports directly or indirectly connect the DHCP server should be configured as trust port on the network device between the DHCP Client and the Server, including the MLAG peer devices.
- DHCP relay configurations should be configured identically on both MLAG peer devices.

DHCP snooping and DHCP relay in MLAG topology present the following characteristics:

1. DHCP snooping binding table and DHCP relay table of the MLAG member ports will be synchronized to the associated member ports on MLAG peer device.
2. If both the MLAG configuration consistency check as well as the DHCP snooping configuration consistency check pass, the MLAG system syncs the DHCP snooping binding table and DHCP relay table; If any of the MLAG or DHCP snooping configuration consistency check fails, the DHCP binding table entries will be cleared.
3. DHCP snooping binding table and DHCP relay table of the single-homed ports will not be synchronized to the MLAG peer device.
4. When receiving a DHCP message (especially for broadcast messages), the message will be forwarded by DHCP relay, and at the same time flooded in the same VLAN.
5. MLAG flood control module processes DHCP packets just like other packets: When the MLAG member port is in the FULL state, DHCP packets received from the peer link port cannot be forwarded out from the MLAG member port; However, when the MLAG interface state changes to AS_LOCAL, the prohibition is lifted.
6. The format of DHCP Option 82 sub-options remote ID and circuit ID is fixed in MLAG topology,

- MLAG domain MAC address is used to fill in remote ID field.
- MLAG Link ID and Port Index are used for circuit ID field with an offset, see the following table for details:

	MLAG Port	Non-MLAG Port
MLAG Node 0	512 + MLAG Link ID	Local Port Index
MLAG Node 1	512 + MLAG Link ID	1024 + Local Port Index

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

VRRP

The DHCP relay feature can be implemented in the VRRP network, allowing the VRRP Master and Backup devices to act as the DHCP relay agents.

When configuring DHCP relay in VRRP topology, pay attention to the following points:

- DHCP relay configurations must be identical on both *VRRP Master/Backup* devices, such as the DHCP server address.
- In VRRP topology, DHCP relay only works on the L3 VLAN interface with single IP address and single VRID.
- DHCP relay agent address is required in VRRP topology, and it must be specified as the virtual IP address of the VRRP group. The command **set protocols dhcp relay interface** *<vlan-interface-name>* **relay-agent-address** *<agent-ipv4-address>* can be used to set the *DHCP relay agent address*. It is used to fill in the giaddr field to identify the client gateway in the DHCP relay Discover/Request/Inform/Release/Decline message where the giaddr is zero. For those DHCP messages in which the giaddr isn't zero, the giaddr remains unchanged.
- Dynamic ARP Inspection (DAI) is supported in the Active-Active VRRP mode, but NOT supported in the standard VRRP mode.

Configuration Notes of DHCP

When configuring DHCP snooping and DHCP relay, pay attention to the following notes:

- DHCP relay only works on the L3 VLAN interface with single IP address and single VRID if VRRP is used.
- DHCP relay supports VRF function by binding DHCP client VLAN interface to a specified VRF.
- Inter-VRF routing isn't support by DHCP relay.
- Dynamic ARP Inspection (DAI) is supported in the Active-Active VRRP mode, but NOT supported in the standard VRRP mode.
- Enable IP routing function before using DHCP relay.
- When a DHCP Offer/Ack/Nak message with Option 82 is received, Option 82 is removed before the message is forwarded.
- The DHCP snooping function is only practicable to the clients directly connected in the local L2 domain, rather than connected through a router.
- There will be compatibility issues with DHCP features when upgrading from a version before PICOS 3.7.0, so upgrading from a version before 3.7.0 to this version is not supported.
- When configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Configuring DHCP Server (IPv4)

- Introduction
- Configuration Notes
- Configuring DHCP Server
  - Procedure
- Configuration Example
  - Networking Requirements
  - Procedure
  - Verify the Configuration

Introduction

Dynamic Host Configuration Protocol (DHCP) is a protocol that dynamically configures and centrally manages the network parameters of the hosts based on TCP / IP protocol, which can be used to:

- Dynamically assign IP addresses to network hosts. Assign an IP address to a host via DHCP with an expiration time (often called a lease time). The default lease time is one hour.
- Provide other network parameters for network hosts, such as the IP address of the DNS server, domain name information and default gateway address.

Configuration Notes

Pay attention to the following points when configuring DHCP server:

- Enabling DHCP client, DHCP relay or DHCP server functions in block VLAN is not supported.
- Enabling DHCP client, DHCP snooping/relay and DHCP server functions in the same VLAN is not supported. Where DHCP snooping and DHCP relay don't have this limitation, they can be enabled in the same VLAN.
- Enabling both DHCP relay and DHCP server functions in the same VRF is supported.
- If both DHCP server and DHCP relay are deployed on the same switch, don't use the VLAN interface enabled with DHCP server to connect to the remote DHCP server.
- DHCP server feature supports only IPv4, and doesn't support IPv6.
- DHCP server supports VRF by binding the address pool and the VLAN interface (which is connected to the DHCP client side) to the same VRF.
- One VRF will run a DHCP server instance. So different VRFs will have different DHCP server instances.
- In each VRF, at most 1000 DHCP clients are allowed.
- Multiple address pools can be configured in the same VRF, but there cannot be address overlap between individual pools. However, address pools in different VRFs do not have this restriction.
- When multiple address ranges are configured under one address pool, there should be no address overlap between these ranges.
- The default router is the default gateway of the DHCP client, which is required to be on the same network segment as the address pool.
- In a VRRP topology, if the DHCP server function is enabled, the address pool configured on the master cannot overlap with that configured on the backup switch.
- Adding, deleting and modifying any parameter in the DHCP address pool will result in the deletion of DHCP server binding table in this VRF.

Configuring DHCP Server

Procedure

Step 1 Create an address pool and specify the IPv4 network segment that can be dynamically allocated to the DHCP clients.

set protocols dhcp server pool <*pool-name*> **network** <*IPv4Net*>

Step 2 Configure the VLAN interface connected to the DHCP client.

set vlans vlan-id <*vlan-id*>

set vlans vlan-id <*vlan-id*> l3-interface <*interface-name*>

set l3-interface vlan-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*number*>

Step 3 (Optional) Associate the VLAN interface with a VRF.

If you want to configure the DHCP server for a user-defined VRF, you need to configure this step.

set l3-interface vlan-interface <*interface-name*> **vrf** <*vrf-name*>

Step 4 (Optional) Configure the lower and upper boundaries of an address range in the address pool.

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **low** <*ipv4-address*>

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **high** <*ipv4-address*>

NOTEs:

- The address range is optional. If not configured, it means that all the IP addresses in the address pool are available for address assignment. However, if configured, only addresses in the range can be used for address assignment.
- When multiple address ranges are configured under an address pool, there should be no address overlap between different ranges.

Step 5 (Optional) Configure a lease time for the IP addresses in an address pool.

set protocols dhcp server pool <*pool-name*> **lease-time** <*lease-time*>

By default, the lease time is 60 minutes.

Step 6 (Optional) In a DHCP relay scenario, the following command needs to be used to enable the DHCP server function on the Layer 3 interface.

set protocols dhcp server interface <*interface-name*> **disable** <**true** | **false**>

Step 7 (Optional) Configure the IP address of the DNS server and domain name for the DHCP address pool.

a) Configure the IP address of the DNS server.

set protocols dhcp server pool <*pool-name*> **dns-server** <*dns-server-ip*>

NOTEs:

- By default, no DNS server IP address is configured in a DHCP address pool.
- Each address pool can be configured with a maximum of eight DNS server IP addresses.

b) Configure a domain name for the DHCP clients.

set protocols dhcp server pool <*pool-name*> **domain-name** <*domain-name*>

Step 8 (Optional) Configure a default gateway address for the DHCP clients.

set protocols dhcp server pool <*pool-name*> **default-router** <*router-ip address*>

Step 9 (Optional) Assign a DHCP address pool to a VRF.

set protocols dhcp server pool <*pool-name*> **vrf** <*vrf-name*>

By default, no VRF is configured for an address pool, the address pool belongs to the default VRF.

Step 10 (Optional) Configure the IP address for the TFTP server. After the client sends request packets to the DHCP server, the TFTP server with this IP address will be replied.

set protocols dhcp server pool <*pool-name*> **tftp-server** <*tftp-server-ip*>

Step 11 (Optional) Configure the IP address for the Syslog server. After the client sends request packets to the DHCP server, the Syslog server with this IP address will be replied.

set protocols dhcp server pool <*pool-name*> **log-server** <*log-server-ip*>

Step 12 (Optional) Configure the file name with path on the TFTP server or the file name with URL on the HTTP server. After the client sends request packets to the DHCP server, the file name with path or URL will be replied.

set protocols dhcp server pool <*pool-name*> **bootfile-name** {**file-path** <*file-path*> | **url** <*url*>}

Step 13 (Optional) Configure the file name with path on the TFTP server or the file name with URL on the HTTP server. After the client sends request packets to the DHCP server, the file name with path or URL will be replied.

set protocols dhcp server pool <*pool-name*> **bootfile-name** {**file-path** <*file-path*> | **url** <*url*>}

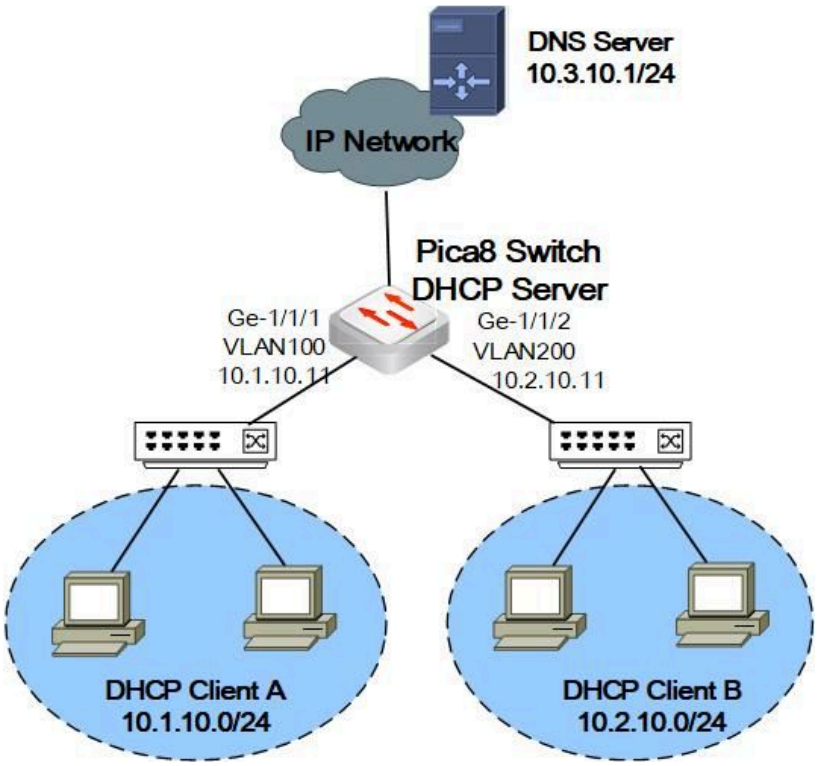
NOTEs:

- If commands of **set protocols dhcp server pool tftp-server** and **set protocols dhcp server pool bootfile-name url** are both configured, the TFTP server is valid, and error prompt appears for the script in the TFTP server cannot be obtained.
- Commonly, the commands of TFTP server and Syslog server are applied for the ZTP function. For details of ZTP, see Zero Touching Provisioning (ZTP).
- By default, no TFTP and Syslog server IP address is configured in a DHCP address pool.
- Each address pool can be respectively configured with one TFTP server address and one Syslog server address.
- If you configure the IP address of TFTP server or Syslog server through ZTP provision script, it will be used in preference to the configurations in the DHCP server.

Configuration Example

Networking Requirements

Figure 1. DHCP Server Configuration Example



As shown in **Figure 1**, an enterprise has planned two network segments for the office terminals. PCs in the network segment 10.1.10.0/24 are the fixed terminals, and the network segment 10.2.10.0/24 is used for temporary users accessing to the network. To facilitate unified administration, the enterprise terminals can automatically obtain IP address and DNS server address from the DHCP server.

By configuring DHCP server on Pica8 switch, IP address and DNS server address can be dynamically assigned to the terminals in the two separate network segments of the enterprise. Among them, the PCs in network segment 10.1.10.0/24 are the fixed office terminal, and the IP lease time is 30 days; the network segment 10.2.10.0/24 provides temporary accesses to the network for business travelers, and the IP lease time is 2 days.

Procedure

Step 1 Configure the VLAN interface connected to the DHCP client.

```
admin@Xorplus# set vlans vlan-id 100
admin@Xorplus# set vlans vlan-id 200
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@Xorplus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 200
admin@Xorplus# set vlans vlan-id 100 l3-interface vlan100
admin@Xorplus# set vlans vlan-id 200 l3-interface vlan200
admin@Xorplus# set l3-interface vlan-interface vlan100 address 10.1.10.11 prefix-length 24
admin@Xorplus# set l3-interface vlan-interface vlan200 address 10.2.10.11 prefix-length 24
```

Step 2 Create two address pools and specify the IPv4 network segment that can be dynamically allocated to the DHCP clients.

```
admin@Xorplus# set protocols dhcp server pool pool1 network 10.1.10.0/24
admin@Xorplus# set protocols dhcp server pool pool2 network 10.2.10.0/24
```

Step 3 Configure the lease time for the IP addresses in the address pool.

```
admin@Xorplus# set protocols dhcp server pool pool1 lease-time 43200
admin@Xorplus# set protocols dhcp server pool pool2 lease-time 2880
```

By default, the IP address lease is one hour.

Step 4 Configure the IP address of the DNS server and domain name for the DHCP clients.

a) Configure the IP address of the DNS server for each address pool.

By default, no DNS server is configured in an address pool.

b) Configure domain name for the DHCP clients.

```
admin@Xorplus# set protocols dhcp server pool pool1 domain-name company.com
```

Verify the Configuration

- The IP address and DNS server address of the 10.1.10.0/24 network segment can be obtained from the DHCP server by the PCs in the zone of DHCP client A, and the IP address and DNS server address of the 10.2.10.0/24 network segment can be obtained from the DHCP server by the PCs in the zone of DHCP client B.
- Run the command **run show dhcp server binding** on the switch to view the allocated IP address binding information.

```
admin@Xorplus# set protocols dhcp server pool pool1 dns-server 10.3.10.1
admin@Xorplus# set protocols dhcp server pool pool2 dns-server 10.3.10.1
```

```
admin@Xorplus# run show dhcp server binding
2 bound clients

IP address       MAC address          Server        Interface
10.1.10.89       00:0a:12:00:12:12    10.1.10.11    vlan100
10.2.10.88       00:0a:12:00:12:34    10.2.10.11    vlan200

admin@Xorplus# run show dhcp server binding interface vlan100
Client Interface: vlan100
    MAC address:          00:0a:12:00:12:12
    Client IP Address:      10.1.10.89

    DHCP Options :
    Name: dhcp-lease-time, Value: 43200 minutes
    Name: name-server, Value: [10.3.10.1]
    Name: server-identifier, Value: 10.1.10.11
    Name: router, Value: [ 10.1.10.11 ]
    Name: domain-name, Value: company.com
```

Configuring DHCP Relay

- Configuring DHCP Relay (IPv4)
- Example for Configuring DHCPv6 Relay
- Example for Configuring DHCP Relay over GRE Tunnel

Configuring DHCP Relay (IPv4)

As DHCP is used to send the request packet during the dynamic acquisition of IP address, DHCP is only applicable to the case where the DHCP client and the server are on the same subnet.

For this reason, you have to set up a DHCP server on each network segment for dynamic host configuration, which is obviously very uneconomical. The introduction of DHCP relay function solves this problem: the client can communicate with the DHCP server of other network segment through DHCP relay agent, to obtain the IP address finally. In this way, DHCP clients on multiple networks can share the same DHCP server, which saves the cost as well facilitates centralized management.

Note that: the configuration and processing of DHCP relay function have nothing to do with the DHCP snooping trust port.

NOTE:

- DHCP relay supports VRF function by binding DHCP client VLAN interface to a specified VRF.
- When configuring DHCP relay, the VLAN interface connected to the clients and the VLAN interface connected to the DHCP server should be in the same VRF.

Procedure

Step 1 Configure VLAN.

a). Configure VLAN ID.

set vlans vlan-id <*vlan-id*>

b). Add an interface to the VLAN.

set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

c). Associate a Layer 3 interface with a VLAN.

set vlans vlan-id <*vlan-id*> **l3-interface** <*interface-name*>

d). Configure the IP address for the VLAN interface to implement Layer 3 connectivity.

set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

Step 2 Enable IP routing function when using DHCP relay.

set ip routing enable <true | **false>**

Step 3 Enable the DHCP relay function on the L3 VLAN interface connected to the client.

set protocols dhcp relay interface <*vlan-interface-name*> **disable** <**true** | **false**>

Step 4 Configure the IP address of the DHCP server.

set protocols dhcp relay interface<*vlan-interface-name*> **dhcp-server-address** <*ipv4-address*>

Note that the VLAN interface is L3 VLAN interface that connected to the client.

Step 5 (Optional) Configure the IP address of the DHCP relay agent.

set protocols dhcp relay interface <*vlan-interface-name*> **relay-agent-address** <*agent-ipv4-address*>

NOTE:

DHCP relay agent address is a required configuration in VRRP topology, when the VRRP Master/Backup devices are used as the DHCP relay agents, you must configure the DHCP relay agent address to the virtual IP address of the VRRP group.

The interface name here should be configured with the L3 VLAN interface which is enabled with DHCP relay and VRRP group.
However, in a non-VRRP topology, there's no need to configure the DHCP relay agent address. By default, the system sets the IP address of the L3 VLAN interface that enabled DHCP relay as the DHCP relay agent address.

Step 6 (Optional) Configure the DHCP relay Option 82 policy and the sub-options.

set protocols dhcp relay interface <*vlan-interface-name*> **option82-policy** <**drop | keep | insert | replace**>

set protocols dhcp relay option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp relay option82 remote-id <**system-mac | hostname**>

Step 7 (Optional) Enable Option 82 trust-all function for DHCP relay.

set protocols dhcp relay option82 trust-all <**true | false**>

Step 8 (Optional) Configuring DHCP relay in a VRF.

To enable DHCP relay in a VRF, the configuration method is to bind the DHCP client side VLAN interface to a user-defined VRF by using the following command.

set l3-interface vlan-interface <*interface-name*> **vrf** <*vrf-name*>

By default, the VLAN interface is bound to the default VRF if not specified to a user-defined VRF.

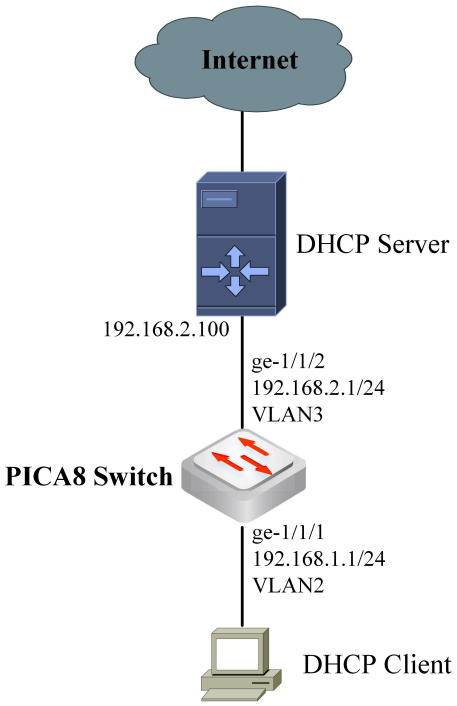
If DHCP relay is deployed in a VRF, this step is required. The VLAN interface connected to the clients and the VLAN interface connected to the DHCP server should be in the same VRF. Otherwise, the DHCP client cannot obtain the IP address normally.

Configuration Example

Networking Requirements

- On PICA8 Switch, the interfaces ge-1/1/1 belongs to VLAN 2 and ge-1/1/2 belongs to VLAN 3.
- The L3 VLAN interface associated with VLAN 2 is vlan-2, the interface IP is 192.168.1.1/24; The L3 VLAN interface associated with VLAN 3 is vlan-3, the interface IP is 192.168.2.1/24.
- Enable DHCP relay function on the L3 VLAN interface vlan-2.
- The IP address of DHCP server is 192.168.2.100.

Figure 1 DHCP Relay Network



Procedure

Step 1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 192.168.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 192.168.2.1 prefix-length 24
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
```

Step 2 Enable IP routing function when using DHCP relay.

```
admin@XorPlus# set ip routing enable true
```

Step 3 Enable the DHCP relay function on L3 VLAN interface vlan-2.

```
admin@XorPlus# set protocols dhcp relay interface vlan-2 disable false
```

Step 4 Configure the IP address of DHCP server 192.168.2.100.

```
admin@XorPlus# set protocols dhcp relay interface vlan-2 dhcp-server-address 192.168.2.100
```

Step 5 Commit the configuration.

```
admin@XorPlus# commit
```

Step 6 Verify the configuration.

- After the configuration is complete, run the **show protocols dhcp relay** command to view the configuration of DHCP relay.

```
admin@Xorplus# show protocols dhcp relay
    interface vlan-2 {
        disable: false
        dhcp-server-address 192.168.2.100
        relay-agent-address: 192.168.1.1
   }
```

- DHCP client can obtain the IP address normally.

Example for Configuring DHCPv6 Relay

A DHCPv6 relay agent enables the DHCPv6 client and server on different links to exchange DHCPv6 messages. The DHCPv6 relay agent forwards DHCP messages to the destination DHCPv6 server on a different network segment. DHCPv6 clients on multiple networks can share one DHCPv6 server.

Multiple DHCPv6 relays can be configured between the DHCPv6 client and server. If a device functions as a DHCPv6 relay and it is directly connected to the DHCPv6 server then you need to specify the IPv6 address of the DHCPv6 server when enabling the DHCPv6 relay feature. If the DHCPv6 relay device is connected to a next-hop relay device then you need to specify the IPv6 address of the next-hop relay device. All the intermediate relay devices are configured with the next-hop device's IPv6 address until the server's IPv6 address is configured on the last relay device in the chain which has a direct connection to the DHCP6 server.

> **NOTE:**
> DHCPv6 relay supports VRF function by binding the VLAN interface to a specified VRF.

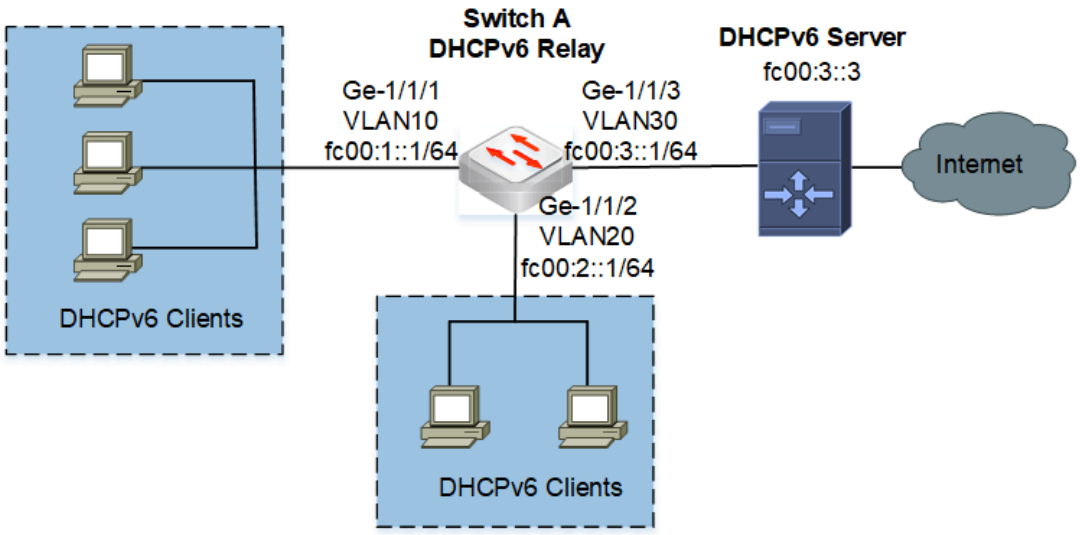
The following configuration example shows how to configure a DHCPv6 relay to assign IPv6 addresses to the clients in multiple network segments.

- Networking Requirements
  - Figure 1. Networking diagram for configuring DHCPv6 relay
- Procedure

Networking Requirements

As shown in Figure 1, the DHCPv6 clients in two network segments fc00:1::/64 and fc00:2::/64 want to dynamically obtain IPv6 addresses from the DHCPv6 server when the DHCPv6 server and clients are in different subnets. The addresses fc00:1::1/64 and fc00:2::1/64 on Switch A are used as the gateway addresses of the clients in network segments fc00:1::/64 and fc00:2::/64.

Figure 1. Networking diagram for configuring DHCPv6 relay



Configure the DHCPv6 relay function on Switch A to forward DHCPv6 packets between the DHCPv6 server and clients so that the clients can dynamically obtain IPv6 addresses.

Switch A is used as a DHCPv6 relay device. DHCPv6 clients can communicate with the DHCPv6 server in a different subnet through DHCPv6 relay to obtain IPv6 addresses from the DHCPv6 server's IPv6 address pool and other configuration information. Using a common DHCPv6 server in this manner not only saves the cost but also facilitates centralized management.

To enable DHCPv6 relay, there are two key steps that should be configured:

1. Enable the DHCPv6 relay function on L3 VLAN interface.
2. Configure the IP address of DHCPv6 server or the next-hop DHCPv6 relay device.

Procedure

Step 1 Configure VLAN interfaces.

```
admin@Xorplus# set vlans vlan-id 10
admin@Xorplus# set vlans vlan-id 20
admin@Xorplus# set vlans vlan-id 30
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@Xorplus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@Xorplus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@Xorplus# set vlans vlan-id 10 l3-interface vlan10
admin@Xorplus# set vlans vlan-id 20 l3-interface vlan20
```

```
admin@Xorplus# set vlans vlan-id 30 l3-interface vlan30
admin@Xorplus# set l3-interface vlan-interface vlan10 address fc00:1::1 prefix-length 64
admin@Xorplus# set l3-interface vlan-interface vlan20 address fc00:2::1 prefix-length 64
admin@Xorplus# set l3-interface vlan-interface vlan30 address fc00:3::1 prefix-length 64
```

Step 2 Enable IP routing function when using DHCPv6 relay.

```
admin@XorPlus# set ip routing enable true
```

Step 3 Enable the DHCPv6 relay function on L3 VLAN interface vlan10 and vlan20.

```
admin@XorPlus# set protocols dhcp6 relay interface vlan10 disable false
admin@XorPlus# set protocols dhcp6 relay interface vlan20 disable false
```

Step 4 Configure the IP address of DHCPv6 server.

```
admin@XorPlus# set protocols dhcp6 relay interface vlan10 destination fc00:3::3
admin@XorPlus# set protocols dhcp6 relay interface vlan20 destination fc00:3::3
```

Step 5 Configure to advertise RA messages and configure the M flag bit.

```
admin@XorPlus# set l3-interface vlan-interface vlan10 ipv6-nd suppress-ra false
admin@XorPlus# set l3-interface vlan-interface vlan10 ipv6-nd prefix fc00:1::0/64 router-address
admin@XorPlus# set l3-interface vlan-interface vlan10 ipv6-nd managed-config-flag
```

Step 6 Commit the configuration.

```
admin@XorPlus# commit
```

Step 7 Verify the configuration.

- After the configuration is complete, run the show protocols dhcp6 relay command to view the configuration of DHCPv6 relay.

```
admin@XorPlus# show protocols dhcp6 relay
    interface vlan10 {
        disable: false
        destination fc00:3::3
    }
    interface vlan20 {
        disable: false
        destination fc00:3::3
    }
```

- Run the **run show dhcp6 relay-stats** command to view DHCPv6 relay running status and statistics.

```
admin@Xorplus# run show dhcp6 relay-stats
Vif Name        Rx        Tx
-----------------------------------
vlan10          6866      1626
vlan20          2455      896
Total 2 Vif(s) enabled with DHCP6 relay
```

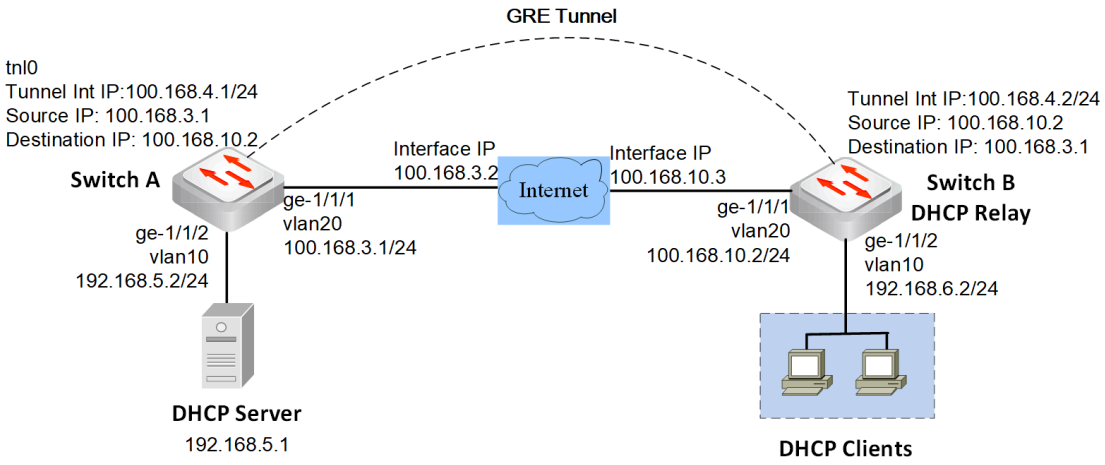
- DHCPv6 client can obtain the IP address normally.

Example for Configuring DHCP Relay over GRE Tunnel

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Verifying the Configuration

Networking Requirements

Figure 1. DHCP Relay over GRE Tunnel Configuration Example



As shown in **Figure 1**, the DHCP server and DHCP clients are deployed in different areas, and are belonged to different network segments. DHCP server accesses the network through Switch A, DHCP clients access the network through Switch B. In this scenario, DHCP relay needs to be configured on Switch B.

To enable communication between DHCP server and DHCP clients through the public network, a Generic Routing Encapsulation (GRE) tunnel needs to be deployed between Switch A and Switch B.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchA# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@SwitchA# set l3-interface vlan-interface vlan10 address 192.168.5.2 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan20 address 100.168.3.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step3 Configure GRE tunnel name, IP, source IP, destination IP etc.

```
admin@SwitchA# set l3-interface tunnel tnl0 address 100.168.4.1 prefix-length 24
admin@SwitchA# set l3-interface tunnel tnl0 tunnel-mode gre-ip
admin@SwitchA# set l3-interface tunnel tnl0 source 100.168.3.1
admin@SwitchA# set l3-interface tunnel tnl0 destination 100.168.10.2
```

Step4 Create static routes for the GRE tunnel.

```
admin@SwitchA# set protocols static route 192.168.6.0/24 next-hop 100.168.4.2
admin@SwitchA# set protocols static route 100.168.10.0/24 next-hop 100.168.3.2
```

Or we can create the static route using the tunnel name as the next hop.

```
admin@SwitchA# set protocols static interface-route 192.168.6.0/24 interface tnl0
```

Step5 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@SwitchB# set l3-interface vlan-interface vlan10 address 192.168.6.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan20 address 100.168.10.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step3 Configure GRE tunnel name, IP, source IP and destination IP.

```
admin@SwitchB# set l3-interface tunnel tnl0 address 100.168.4.2 prefix-length 24
admin@SwitchB# set l3-interface tunnel tnl0 tunnel-mode gre-ip
admin@SwitchB# set l3-interface tunnel tnl0 source 100.168.10.2
admin@SwitchB# set l3-interface tunnel tnl0 destination 100.168.3.1
```

Step4 Create static routes for the GRE tunnel.

```
admin@SwitchB# set protocols static route 192.168.3.0/24 next-hop 100.168.10.3
admin@SwitchB# set protocols static route 192.168.5.0/24 next-hop 100.168.4.1
```

Or we can create the static route using the tunnel name as the next hop.

```
admin@SwitchB# set protocols static interface-route 192.168.5.0/24 interface tnl0
```

Step5 Enable the DHCP relay function on VLAN interface vlan10 and specifies the DHCP server address for the relay.

```
admin@SwitchB# set protocols dhcp relay interface vlan10 disable false
admin@SwitchB# set protocols dhcp relay interface vlan10 dhcp-server-address 192.168.5.1
```

Step6 Commit the configuration.

```
admin@SwitchB# commit
```

Verifying the Configuration

- After the configuration is complete, run the **show protocols dhcprelay** command to view the configuration of DHCP relay.

```
admin@SwitchB# show protocols dhcp relay
    interface vlan10 {
        disable: false
        dhcp-server-address 192.168.5.1
   }
```

- Run command **run show l3-interface tunnel** to display information about the GRE tunnel interface.

```
admin@SwitchB# run show l3-interface tunnel tnl0
tnl0         State:UP
            Tunnel Source: 100.168.3.1
            Tunnel Destnation:: 100.168.10.2
            Tunnel protocol/transport: gre-ip
            Inet addr: 100.168.4.1
```

```
Traffic statistics:
  5 sec input rate IPv4 1400 packets/sec, IPv6 0 packets/sec
  5 sec forwarding rate IPv4 28 packets/sec, IPv6 0 packets/sec
  IPv4 Input Packets.....................28
  IPv4 Forwarding Packets.....................5
  IPv6 Input Packets.....................0
  IPv6 Forwarding Packets.....................0
```

- DHCP clients can obtain the IP address normally.

Configuring DHCP Snooping

- Configuring DHCP Snooping (IPv4)
- Configuring DHCPv6 Snooping (IPv6)

Configuring DHCP Snooping (IPv4)

DHCP snooping creates a binding table, which includes the client IP address, MAC address, VLAN ID, physical port and the lease time. DHCP snooping is disabled by default. The steps below explain how to enable DHCP snooping and configure the trust port (by default all the ports are untrusted ports), DHCP snooping binding file and the delay timer for writing the DHCP snooping entries from memory to the binding file, and how to configure DHCP snooping Option 82 policy.

Procedure

Step 1 Configure DHCP snooping on a VLAN.

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

> **NOTE：**
>
> DHCP snooping should be enabled in the VLAN, it takes effect only on DHCP messages received from interfaces in this VLAN. Packets that are not received from this VLAN won't be processed by DHCP snooping module and will be processed and forwarded as ordinary packets.

Step 2 Configure the interface connected to the DHCP server as DHCP snooping trusted interface.

set protocols dhcp snooping trust-port <*interface-name*>

> **NOTE：**
>
> - The port can be either physical port or aggregated port.
> - By default, all the ports are untrusted ports.
> - When DHCP snooping is enabled in a VLAN without configuring the trust interface, the DHCP packets received from the DHCP server in this VLAN will be dropped.

Step 3 (Optional) Configure the DHCP snooping binding file and the delay timer for writing the DHCP snooping entries from memory to the binding file.

set protocols dhcp snooping binding file <*file-path*>
set protocols dhcp snooping binding write-delay <*write-delay-timer*>

Step 4 (Optional) Configure the DHCP snooping Option 82 policy and the sub-options.

set protocols dhcp snooping vlan <*vlan-id*> **option82-policy** <**drop | keep | insert | replace**>

set protocols dhcp snooping option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp snooping option82 remote-id <**system-mac | hostname**>

Step 5 (Optional) Enable Option 82 trust-all function for DHCP snooping.

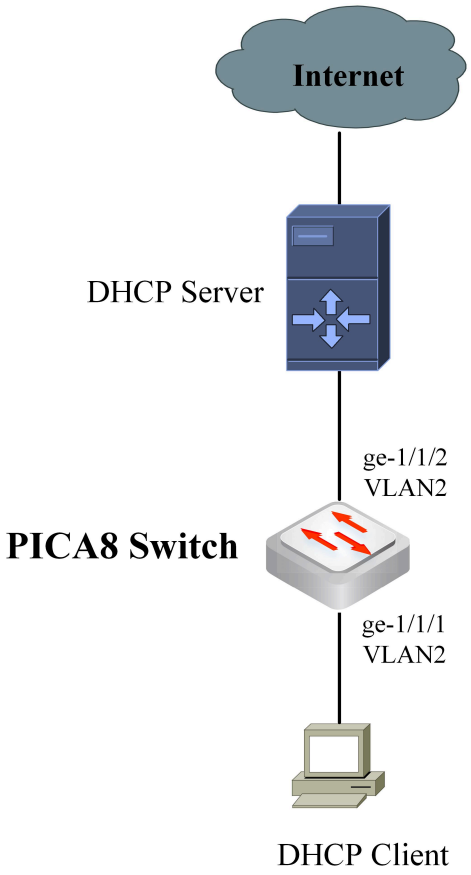
set protocols dhcp snooping option82 trust-all <**true | false**>

Configuration example

Networking Requirements

- On PICA8 Switch, the interfaces ge-1/1/1 and ge-1/1/2 are in VLAN 2.
- Enable DHCP snooping on VLAN 2.
- Configure the interface connected to the DHCP server (ge-1/1/2) as the DHCP snooping trust interface.

Figure 1 DHCP Snooping Networks



Procedure

Step 1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
```

Step 2 Configure DHCP snooping on VLAN 2.

```
admin@XorPlus#set protocols dhcp snooping vlan 2 disable false
```

Step 3 Configure the interface connected to the DHCP server as DHCP snooping trusted interface.

```
admin@XorPlus# set protocols dhcp snooping trust-port ge-1/1/2
```

Step 4 (Optional) Configure /tmp/run/dhcp_bind as the DHCP snooping binding file and the value of delay timer for writing the DHCP snooping entries from memory to the binding file is 30s.

```
admin@XorPlus# set protocols dhcp snooping binding file /tmp/run/dhcp_bind
admin@XorPlus# set protocols dhcp snooping binding write-delay 30
```

Step 5 Commit the configuration.

```
admin@XorPlus# commit
```

Step 6 Verify the configuration.

- After the configuration is complete, run the **run show dhcp snooping** command to view the DHCP snooping binding table.

```
admin@Xorplus# run show dhcp snooping binding
Total count:     1
MAC Address         IP Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------------
14:18:77:18:2c:b9   100.1.1.1      ge-1/1/1        2         599/600
```

- DHCP client can obtain the IP address normally.

Configuring DHCPv6 Snooping (IPv6)

DHCPv6 snooping creates a binding table, which includes the client IP address, MAC address, VLAN ID, physical port and the lease time. DHCPv6 snooping is disabled by default. The steps below explain how to enable DHCPv6 snooping and configure the trust port (by default all the ports are untrusted ports), DHCPv6 snooping binding file and the delay timer for writing the DHCPv6 snooping entries from memory to the binding file, and how to configure DHCPv6 snooping Option policy.

Procedure

Step 1 Configure DHCPv6 snooping on a VLAN.

set protocols dhcp6 snooping vlan <*vlan-id*> **disable** <**true** | **false**>

NOTE：

- DHCPv6 relay and DHCPv6 snooping cannot be configured on the same VLAN.
- DHCPv6 snooping should be enabled in the VLAN, it takes effect only on DHCPv6 messages received from interfaces in this VLAN. Packets that are not received from this VLAN won't be processed by DHCPv6 snooping module and will be processed and forwarded as ordinary packets.

Step 2 Configure the interface connected to the DHCP server as DHCPv6 snooping trusted interface.

set protocols dhcp6 snooping trust-port <*interface-name*>

NOTE：

- The port can be either physical port or aggregated port.
- By default, all the ports are untrusted ports.
- When DHCPv6 snooping is enabled in a VLAN without configuring the trust interface, the DHCPv6 packets received from the DHCP server in this VLAN will be dropped.

Step 3 (Optional) Configure the DHCPv6 snooping binding file and the delay timer for writing the DHCPv6 snooping entries from memory to the binding file. For non-X86 devices, the path of the binding file is **/mnt/open/dhcp6_bind**; for X86 devices, the binding file path should not be under **/tmp**.

set protocols dhcp6 snooping binding file <*file-path*>
set protocols dhcp6 snooping binding write-delay <*write-delay-timer*>

Step 4 (Optional) Configure the DHCPv6 snooping Option policy and the sub-options.

set protocols dhcp6 snooping vlan <*vlan-id*> **option-policy** <**drop | keep | insert | replace**>

set protocols dhcp6 snooping option18 interface-id <port-index | port-name | port-description>

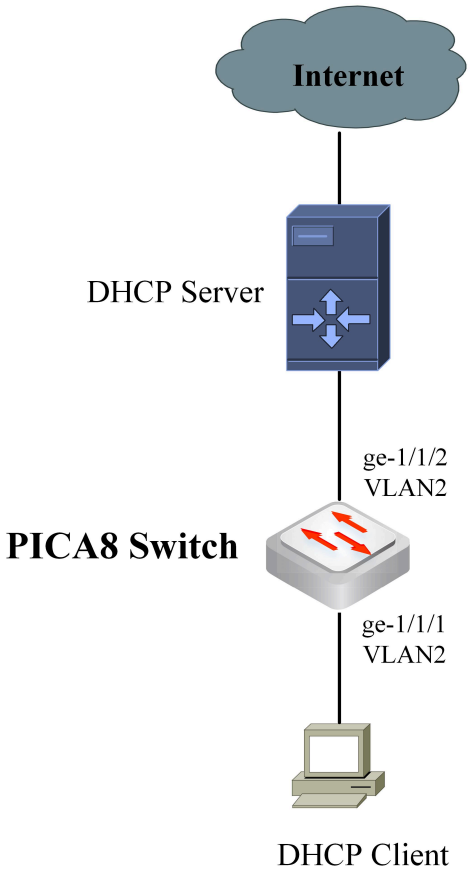
set protocols dhcp6 snooping option37 remote-id <*remote-id*>

Configuration example

Networking Requirements

- On PICA8 Switch, the interfaces ge-1/1/1 and ge-1/1/2 are in VLAN 2.
- Enable DHCPv6 snooping on VLAN 2.
- Configure the interface connected to the DHCP server (ge-1/1/2) as the DHCPv6 snooping trust interface.

Figure 1 DHCPv6 Snooping Networks



Procedure

Step 1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
```

Step 2 Configure DHCPv6 snooping on VLAN 2.

```
admin@XorPlus#set protocols dhcp6 snooping vlan 2 disable false
```

Step 3 Configure the interface connected to the DHCP server as DHCPv6 snooping trusted interface.

```
admin@XorPlus# set protocols dhcp6 snooping trust-port ge-1/1/2
```

Step 4 (Optional) Configure /tmp/run/dhcpv6_bind as the DHCPv6 snooping binding file and the value of delay timer for writing the DHCPv6 snooping entries from memory to the binding file is 30s.

```
admin@XorPlus# set protocols dhcp6 snooping binding file /mnt/open/dhcp6_bind
admin@XorPlus# set protocols dhcp6 snooping binding write-delay 30
```

Step 5 Commit the configuration.

```
admin@XorPlus# commit
```

Step 6 Verify the configuration.

- After the configuration is complete, run the **run show dhcp6 snooping binding** command to view the DHCPv6 snooping binding table.

```
admin@Xorplus# run show dhcp6 snooping binding
Total count:     1
MAC Address         IPv6 Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------------
14:18:77:18:2c:b9   100::1:1:1       ge-1/1/1        2         599/600
```

- DHCPv6 client can obtain the IPv6 address normally.

Typical Configuration Example for DHCP Relay and DHCP Snooping

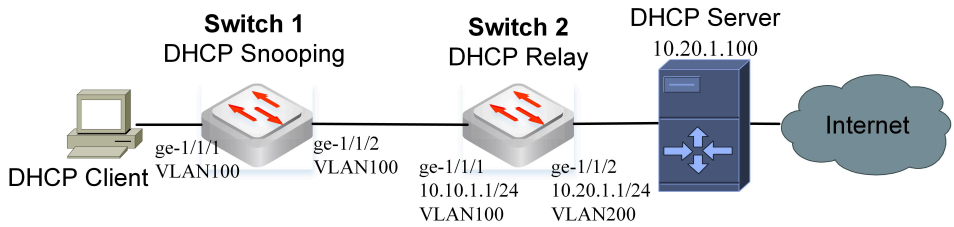
- Networking Requirements
- Procedure
  - Switch 1
  - Switch 2
- Verify the Configuration

Networking Requirements

As shown in figure 5, Switch 1 is a Layer 2 device and Switch 2 is the gateway that acts as a DHCP relay agent to forward DHCP packets between DHCP client and DHCP server, allowing the DHCP client to get configuration parameters such as IP address from the DHCP server.

In order to provide better service to DHCP clients, network administrator can configure DHCP snooping feature on Switch 1 to implement DHCP attack prevention.

Figure 1 User Topology of DHCP Snooping and DHCP Relay



Configure the DHCP Snooping and DHCP Relay by completing the following tasks on each Switch 1 and Switch 2:

- Switch 1 is a Layer 2 device, the interfaces ge-1/1/1 and ge-1/1/2 belong to VLAN 100.
- On Switch 1, enable DHCP snooping in VLAN 100 and configure the interface ge-1/1/2 as the DHCP snooping trust interface.
- On Switch 2, ge-1/1/1 interface belongs to VLAN 100, the IP address of the associated L3 VLAN interface is 10.10.1.1/24; ge-1/1/2 interface belongs to VLAN 200, the IP address of the associated L3 VLAN interface is 10.20.1.1/24.
- Enable DHCP relay on Switch 2 on the L3 VLAN interface VLAN100.
- DHCP server and DHCP relay agent are in the same subnet. The IP address of the DHCP server is 10.20.1.100.

Procedure

Switch 1

Step 1 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 100
admin@Switch1# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@Switch1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100
```

Step 2 Enable DHCP snooping on VLAN 100.

```
admin@Switch1#set protocols dhcp snooping vlan 100 disable false
```

NOTE:

The DHCP snooping function is only practicable to the clients directly connected to the local L2 domain, rather than connected through a router.

Step 3 Configure the interface ge-1/1/2 as DHCP snooping trust interface.

```
admin@Switch1# set protocols dhcp snooping trust-port ge-1/1/2
```

Step 4 Commit the configuration.

```
admin@Switch1# commit
```

Switch 2

Step 1 Configure the VLANs.

```
admin@Switch2# set vlans vlan-id 100
```

```
admin@Switch2# set vlans vlan-id 200
admin@Switch2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@Switch2# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 200
admin@Switch2# set vlans vlan-id 100 l3-interface VLAN100
admin@Switch2# set vlans vlan-id 200 l3-interface VLAN200
admin@Switch2# set l3-interface vlan-interface VLAN100 address 10.10.1.1 prefix-length 24
admin@Switch2# set l3-interface vlan-interface VLAN200 address 10.20.1.1 prefix-length 24
```

Step 2 Enable IP routing function when using DHCP relay.

```
admin@Switch2# set ip routing enable true
```

Step 3 Enable DHCP relay on the L3 VLAN interface VLAN100.

```
admin@Switch2#set protocols dhcp relay interface VLAN100 disable false
```

Step 4 Configure the IP address for the DHCP server.

```
admin@Switch2#set protocols dhcp relay interface VLAN100 dhcp-server-address 10.20.1.100
```

Step 5 Commit the configuration.

```
admin@Switch2# commit
```

Verify the Configuration

- After the configuration is complete, run the **run show dhcp snooping** command on Switch1 to view the information of DHCP snooping binding table.

```
admin@Switch1# run show dhcp snooping binding
Total count:     1
MAC Address         IP Address     Port           VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------------------
E3:44:56:a2:00:2c   10.10.1.12     ge-1/1/1        100     60/600
```

The format of lease time for the IP address is **Remaining Lease Time/Total Lease Time**.

- DHCP client can obtain the IP address normally.

DHCPv6 Guard Configuration

- Overview of DHCPv6 Guard
- Configuring DHCPv6 Guard
- Example for Configuring DHCPv6 Guard

Overview of DHCPv6 Guard

DHCPv6 Guard is a security mechanism used to protect the DHCPv6 environment from malicious DHCPv6 servers or intermediate devices that adversely affect DHCPv6 clients. It ensures the security and reliability of DHCPv6 services by detecting and blocking unauthorized DHCPv6 traffic.

DHCPv6 Guard works in the following ways:

- Flow measurement: Monitor DHCPv6 traffic on the network, including communication between DHCPv6 servers and clients.
- Authorization verification: Check whether the DHCPv6 traffic is sent from an authorized DHCPv6 server. You can check the source address, the DUID (DHCPv6 Unique Identifier), or other relevant fields of the DHCPv6 message.
- Blocking traffic: If traffic is detected from an unauthorized DHCPv6 server, DHCPv6 Guard blocks it to ensure that the DHCPv6 client does not receive configuration information.

Characteristics

Terminologies

Functional Procedure

- IPv6 Address/Prefix Assignment Process
- Matching Rules for DHCPv6 Guard

Characteristics

- Security: By blocking unauthorized DHCPv6 traffic, DHCPv6 Guard improves the security of DHCPv6 environment and reduces potential security risks.
- Reliability: DHCPv6 Guard improves the reliability of the DHCPv6 service by ensuring that DHCPv6 clients receive configuration information only from authorized DHCPv6 servers.
- Flexibility: DHCPv6 Guard can be configured according to the network environment and security requirements to adapt to different application scenarios

Terminologies

- **Policy**

"Policy" usually refers to a set of rules defined by a network administrator to control and manage how to handle DHCPv6 traffic on the network through DHCPv6 Guard. These policies determine which DHCPv6 servers are considered legitimate while blocking illegal or unauthorized DHCPv6 server activities.

- **IA-Prefix**

“IA-Prefix” is one of the Identity Association (IA) types in DHCPv6 and is used for prefix delegation. Prefix delegation allows a DHCPv6 client to request one or more IPv6 prefixes from a DHCPv6 server to assign IPv6 addresses with these prefixes on the client's subnet.

IA-Prefix Unique Identity Association Identifier (IAID) is an identifier used to distinguish different IAs, generated by the client and sent to the server in a DHCPv6 message. In addition to IAID, IA-Prefix includes parameters such as the length of the requested prefix, T1 and T2 times (for prefix renewal and rebinding).

When the DHCPv6 client needs to assign an IPv6 address to its subnet, it sends a DHCPv6 request message to the DHCPv6 server with the IA-Prefix option. After receiving the request, the server assigns one or more IPv6 prefixes to the client based on its configuration and policies, and sends these information to the client in the DHCPv6 reply message. After receiving the prefixes, the client can use these prefixes to assign IPv6 addresses to other devices on its sub-network.

- **Preference**

“Preference” indicates the relative priority of the DHCPv6 server. When a DHCPv6 client selects a DHCPv6 server among multiple servers, it evaluates the preference values. A server with a higher preference value is the preferred choice.

The preference value is usually an integer, and its range can vary from implementation to implementation. In some implementations, a larger number represents a higher priority, while in others the opposite may be true. If the preference value is not explicitly set, the DHCPv6 server may use the default value, which may vary from implementation to implementation.

The working principle is as follows:

When a DHCPv6 client starts, it sends Solicit message to request available DHCPv6 servers. Multiple DHCPv6 servers may respond with an Advertise message containing their configuration information and preference values. The DHCPv6 client selects the server with the highest priority based on their preference value from responding servers. With the server selected, the DHCPv6 client will send a Request message with the IP address and other configuration information. The selected DHCPv6 server responds by sending a Reply message containing the IP address assigned to the client and other configuration parameters.

- **Device-role**

"Device-role" refers to the functional positioning of network devices in DHCPv6 protocol interactions. The DHCPv6 Guard mechanism involves two main device roles:

1. DHCPv6 Server: The DHCPv6 server responds to client address requests and provides IPv6 addresses, prefixes, and other network configuration parameters. In a DHCPv6 Guard environment, legitimate DHCPv6 servers are clearly identified by the network administrator so that the Guard mechanism can distinguish between legitimate servers and potentially malicious servers.
2. DHCPv6 Client: The DHCPv6 client is a device that requests for IPv6 addresses and network configuration information. A client initiates the DHCPv6 process by sending Solicit message and then receives an Advertise or Reply message from a legitimate DHCPv6 server.

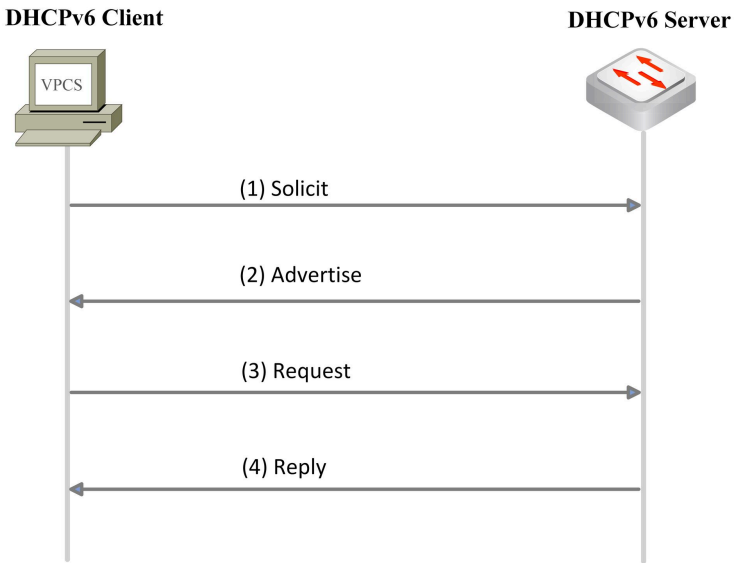
- **Trust-port**

"Trust-port" refers to a port on a network device that is clearly marked to connect to a legitimate DHCPv6 server. If a port is set to Trust-port, all DHCPv6 Advertise and Reply packets received by the port are regarded as legitimate and reliable. The DHCPv6 Guard allows these messages to be forwarded to corresponding clients.

Functional Procedure

IPv6 Address/Prefix Assignment Process

Figure 1. The distribution process of four exchanged messages



The DHCPv6 protocol is used to assign IPv6 addresses to users in a stateful manner, which involves four basic packets, as shown in the figure above.

- Solicit packet: Corresponding to the Discover packet of DHCPv4. The initial request sent by the client to determine the location of the DHCPv6 server. The source port is UDP port 546 and the destination port is 547.

- Advertise packet: Corresponding to the Offer packet of DHCPv4. The response sent by the server declares that it can provide DHCPv6 services and contain an IPv6 address or other configuration information that can be assigned to the client.
- Request packet: Corresponding to the Request packet of DHCPv4. If the client accepts the information provided by the server, it sends this message to request a specific IPv6 address or configuration information.
- Reply packet: Corresponding to the ACK packet of DHCPv4. The final response sent by the server to inform the client that the requested IPv6 address or other configuration information has been assigned.

Matching Rules for DHCPv6 Guard

After receiving DHCPv6 packets, the DHCPv6 Guard processes the packets according to the packet type and port role.

- DHCPv6 request packets: forwarded directly.
- DHCPv6 reply packets: processed according to the port role.

  If the port is trust-port, all packets on the port are directly forwarded.

  If the port role is client, all packets on the port are discarded.

  If the port role is server, the packet will be filtered based on rules.

To ensure the proper functioning of the DHCPv6 Guard feature on network devices, especially when a compliant DHCPv6 server is interfaced, you must designate the device's role within the DHCPv6 Guard policy as a DHCPv6 server. Upon receipt of DHCPv6 response packets, either through a server-bound interface or across a VLAN, the DHCPv6 Guard capability of facilitating packet filtration predicated on these established policies:

- For Advertise messages: The DHCPv6 Guard screens and discards any inappropriate response packets originating from the DHCPv6 server, utilizing Access Control List (ACL) rules for validation. Additionally, responses from the DHCPv6 server that fail to meet predefined priority criteria can also be filtered out.
- For Reply messages: The DHCPv6 Guard filters DHCPv6 Reply packets that contain unauthorized addresses or prefixes through Access Control List (ACL) rules. This ensures that only valid and authorized network configurations are distributed to requesting devices, enhancing network security and stability.

In essence, the DHCPv6 Guard policy implements fine-grained control over DHCPv6 traffic, enabling administrator to maintain a secure and managed network environment by selectively permitting or blocking DHCPv6 packets based on server legitimacy and adherence to configured policies.

The DHCPv6 reply packet can be forwarded to the DHCPv6 client only after passing all DHCPv6 Guard policy checks.

Configuring DHCPv6 Guard

Configuration Notes and Constraints
Procedure

Configuration Notes and Constraints

When configuring DHCPv6 Guard, you should pay attention to the following notes:

- You can configure only one guard policy on an interface. A guard policy can be configured on multiple interfaces.
- By default, the value of device-role is “client”.
- In the guard device-role, if the server and trust-port conflicts with each other, you need to delete one to configure the other.
- If guard device-role is “server”, the default value for preference-min is 0, and preference-max is 255.
- If guard device-role is “client”, all packets in the reply direction are discarded on the port configured with this policy.
- If guard policy is “trust-port”, all DHCPv6 packets on the port configured with the policy are directly forwarded.
- The source-address of matching servers in the guard policy filters only the source address in the Advertise packet but not the source address in the Reply packet.
- DHCPv6 snooping and guard can be placed in the same VLAN. The relay and guard cannot be placed in the same VLAN.
- DHCPv6 Guard does not support the Multi-chassis Link Aggregation Group (MLAG) topology.

Procedure

Step 1 (Optional) Set a matching condition that specifies the source addresses of DHCPv6 servers to matched.

set protocols dhcp6 guard policy <*policy-name*> **match server source-address** <*IPv6Net*>

Step 2 (Optional) The specified IPv6 prefix or network matched by the policy is assigned to the client. The prefix defines the range of IPv6 addresses that can be used by clients.

set protocols dhcp6 guard policy <*policy-name*> **match reply ia-prefix** <*IPv6Net*>

Step 3 (Optional) Set a maximum limit for a preferred value in the DHCPv6 Guard policy to ensure that the DHCPv6 server only considers DHCPv6 responses whose preferred value is lower than or equal to the specified value.

set protocols dhcp6 guard policy <*policy-name*> **preference-max** <*max-value*>

Step 4 (Optional) The minimum limit on the preferred value specified by the user.

set protocols dhcp6 guard policy <*policy-name*> **preference-min** <*min-value*>

Step 5 Configuration options allow different security policies to be defined depending on the source of DHCPv6 messages (server or client), giving more precise control over messages which should be detected, logged, or blocked.

set protocols dhcp6 guard policy <*policy-name*> **device-role** <*server/client*>

Step 6 (Optional) Set a trusted port for DHCPv6 Guard policy to control precisely DHCPv6 messages which should be trusted and processed, limiting trust to messages from a specific port.

set protocols dhcp6 guard policy <*policy-name*> **trust-port**

Step 7 Associate the specified DHCPv6 Guard policy with a specific network interface.

set protocols dhcp6 guard policy <*policy-name*> **interface** <*interface-name*>

Step 8 Commit the configuration.

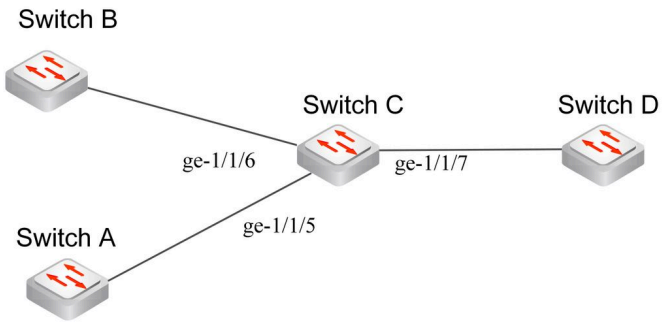
commit

Example for Configuring DHCPv6 Guard

- Network Requirements
- Procedure
- Verifying the Configuration

Network Requirements

Figure 1. DHCPv6 Guard Configuration Example



To maintain the DHCPv6 service properly, the DHCPv6 Guard protocol can be deployed on the device between the DHCPv6 server and the client.

As shown in **Figure 1**, the DHCPv6 Guard is deployed between multiple servers and a single client. You can configure Switch A and Switch B as DHCPv6 servers, configure Switch D as the DHCPv6 client, and configure DHCPv6 guard on Switch C to protect networks from rogue DHCPv6 servers.

Procedure

Switch C

Step 1 Configure policies p1, p2, and p3 on the ports connected to switch A, switch B, and switch D.

```
admin@SwitchC# set protocols dhcp6 guard policy p1 interface ge-1/1/5
admin@SwitchC# set protocols dhcp6 guard policy p2 interface ge-1/1/6
admin@SwitchC# set protocols dhcp6 guard policy p3 interface ge-1/1/7
```

Step 2 Configure a trusted port on the port connected to switch A.

```
admin@SwitchC# set protocols dhcp6 guard policy p1 trust-port
```

Step 3 Configure port roles for the ports that connect to switch B and switch D.

```
admin@SwitchC# set protocols dhcp6 guard policy p2 device-role server
admin@SwitchC# set protocols dhcp6 guard policy p3 device-role client
```

Step 4 Configure multiple filtering policies on the port connected to switch B.

```
admin@SwitchC# set protocols dhcp6 guard policy p2 match server source-address 2001::0/64
admin@SwitchC# set protocols dhcp6 guard policy p2 match reply ia-prefix 2001::0/64
admin@SwitchC# set protocols dhcp6 guard policy p2 preference-max 200
admin@SwitchC# set protocols dhcp6 guard policy p2 preference-min 100
```

Step 5 Commit the configuration.

```
admin@SwitchC# commit
```

Verifying the Configuration

The command **run show dhcp6 guard** can be used to check the configuration information of the DHCPv6 Guard.

```
admin@SwitchC# run show dhcp6 guard
dhcp6 guard policy: p1
  trust Port
  interface: ge-1/1/5
dhcp6 guard policy: p2
  match: server
    source-address: 2001::1/128
      reply ia-prefix: 3001::0/64
  preference-max: 200
  preference-min: 100
  device role: server
  interface: ge-1/1/6
dhcp6 guard policy: p3
  device role: client
  interface: ge-1/1/7
```

As shown in the command output:

- policy p1 is set as a trusted port and applied to port ge-1/1/5.
- Policy p2 checks the packets from the server and allows the packets whose source address is 2001::0/64 to pass and the IA reply packets whose prefix is 2001::0/64 to pass.
- The maximum value of the priority is 200 and the minimum value is 100.
- The role of the port is “server”, which is applicable to port ge-1/1/6.
- Policy p3 defines the port role as client and applies it to port ge-1/1/7.

RFC Lists

The following table lists the RFC documents related to DHCP snooping and DHCP relay.

RFC	Description
RFC 3046	DHCP Relay Agent Information Option
RFC2131	Dynamic Host Configuration Protocol
RFC2132	DHCP Options and BOOTP Vendor Extensions
RFC1534	Interoperation Between DHCP and BOOTP

Default Administrative Distance Values

Select the Best Path

A PicOS system can run multiple routing protocols simultaneously. For example, RIP may be used to distribute routes within our network and BGP to learn external routes. In some situations this can lead to a router learning the same route from more than one routing protocol.

For example, these two routes might be learned:
• Subnet: 128.16.64.0/24, nexthop: 192.150.187.1, learned from BGP via an external peering. AS Path: 123 567 987.
• Subnet: 128.16.64.0/24, nexthop: 10.0.0.2, learned from RIP with metric 13

The longest prefix match rule doesn't help us because the prefix lengths are the same, and the metric used for RIP is not directly comparable against the AS path length or any other attribute attached to a BGP route. So, how do we decide which route to take? A PicOS system uses the concept of administrative distance to determine which route wins. Basically, each routing protocol has a configured "distance," and if a route is heard from two protocols, then the version with the smallest distance wins.

Default Distance Value Table

This table lists the administrative distance default values of the protocols that PicOS supports:

Route Protocol	Default Distance Values
Directly connected	0
Static route	1
External BGP	20
OSPF	110
RIP	120
Internal BGP	200

Hence, in the example above, the route learned from BGP will be preferred.

> ⚠ The administrative distance is fixed in the PicOS system, and cannot be modified.

OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) is a link-state routing protocol that is not proprietary to any vendor or organization. OSPF was developed by IETF (Internet Engineering Task Force), and it is the IGP (Interior Gateway Protocol) recommended by Pica8.

OSPF has evolved through several RFCs. OSPF version 2, which is the current version for IPv4, is defined in RFC 2328. PicOS supports version 2 of the OSPF protocol in L2/L3 mode.

Pica8 PicOS Version 2.6 supports the following OSPF area types:

1. Normal Area
2. Stub Area
3. NSSA (Not-So-Stubby Area)

> **NOTE:**
> Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.

- OSPF Overview
- Basic OSPF Configuration Tasks
- Configuring OSPF Route Summarization
- Basic OSPF Configuration Example
- OSPF Area Type Configuration Example: NSSA, Stub and Standard Areas
- OSPF Stub and NSSA Areas with no-summary
- OSPF Area Range Configuration Guide
- OSPF Route Redistribution and Route Maps
- Example for Configuring OSPF with Different VRFs
- OSPFv3 Configuration Guide
- OSPF Multi-Instance Support
- OSPF GR

OSPF Overview

> **NOTE:**
> Both OSPFv2 and OSPFv3 protocol support VRF.

The high-level operation of OSPF is explained below:

1. OSPF routers send Hello packets out of all OSPF-enabled interfaces. Two routers sharing a common data link become *neighbors.* If they agree on certain parameters in Hello packets.
2. Some neighbors move on and form *adjacencies*, which can be thought of as virtual point-to-point links over which routing information is exchanged.
3. Each OSPF router sends LSAs (link-state advertisements) over all its adjacencies. The LSAs describe the router's neighbors, links, and the state of the links. OSPF defines multiple LSA types to communicate different types of link-state information.
4. When an OSPF router receives an LSA from a neighbor, it adds the LSA to its link-state database. The router also sends a copy of the LSA over all of its adjacencies. The flooding of LSAs throughout an OSPF area enables all routers to have identical link-state databases.
5. When the link-state databases are built, every router runs the Dijkstra's SPF (Shortest Path First) algorithm to calculate the shortest loop-free path to every known subnet. The collection of all paths calculated by the router, with itself as the root, is known as the SPF tree.
6. Each router populates its routing table from its SPF tree.

Basic OSPF Configuration Tasks

To configure OSPF on a PicOS device, complete the tasks described in the following sections.

Configuring OSPF Router ID

The OSPF router ID is a 32-bit value similar to an IP address by which the OSPF router or switch is uniquely identified within the OSPF domain.

Use the following command to configure OSPF router ID:

set protocols ospf router-id *<router-id>*

The following example configures 1.1.1.1 as the OSPF router ID:

```
admin@XorPlus# set protocols ospf router-id 1.1.1.1
admin@XorPlus# commit
Commit OK.
Save done.
```

Do not change the router ID after completing the configuration.

Configuring OSPF Areas

Divide an OSPF domain into areas, which contains the flow of most routing protocol traffic within a single area and reduces the impact of protocol on CPU and memory.

Use the following command to configure OSPF areas:

set protocols ospf area *<area-id>* **area-type** *<type>*

Area ID 0.0.0.0 is reserved for the backbone and each OSPF domain must have the backbone area. All traffic between two non-backbone areas must pass through the backbone area. OSPF area types supported by PicOS are: normal, stub, and NSSA. A normal or standard area in OSPF is one that is configured neither as Stub nor NSSA.

The example that follows demonstrates configuration of three different areas:

Area ID	Area Type
0.0.0.0	Normal
1.1.1.1	Stub
2.2.2.2	NSSA

```
admin@XorPlus# set protocols ospf area 0.0.0.0
admin@XorPlus# set protocols ospf area 1.1.1.1 area-type stub
admin@XorPlus# set protocols ospf area 2.2.2.2 area-type nssa
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring OSPF Interfaces

After configuring OSPF areas, assign a switch interface to the area. Once an interface is assigned to an OSPF area, it will start sending OSPF hello messages.

Use the following command to assign a Layer 3 interface to an OSPF area, where the Layer 3 interface can be the VLAN interface, loopback interface, routed interface or sub-interface:

set protocol ospf interface *<interface-name>* **area {***<ipv4>|<0-4294967295>***}**

The following commands create Layer 3 VLAN interfaces vlan20 and vlan30. The interfaces are given IP addresses and switch ports are assigned to them. Finally, both interfaces are configured to be in the OSPF backbone area according to the table shown below.

VLAN Interface	IP Address / Mask Length	Assigned Switch Interface(s)	OSPF Area
vlan20	10.10.70.10 / 24	ge-1/1/1	0.0.0.0
vlan30	10.10.71.10 / 24	ge-1/1/2	0.0.0.0

```
admin@XorPlus# set vlans vlan-id 20 l3-interface vlan20
admin@XorPlus# set vlans vlan-id 30 l3-interface vlan30
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 30
admin@XorPlus# set l3-interface vlan-interface vlan20 address 10.10.70.10 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan30 address 10.10.71.10 prefix-length 24
admin@XorPlus# set protocols ospf interface vlan20 area 0.0.0.0
```

```
admin@XorPlus# set protocols ospf interface vlan30 area 0.0.0.0
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Additional OSPF Parameters

Fine-tune OSPF operation by configuring additional OSPF interface parameters including hello interval, interface cost, passive interface, BFD, router dead interval, MD5 authentication and MD5 key.

The following example demonstrates how to configure some of the OSPF interface parameters:

```
admin@XorPlus# set protocols ospf interface vlan20 hello-interval 5
admin@XorPlus# set protocols ospf interface vlan20 cost 8
admin@XorPlus# set protocols ospf interface vlan20 dead-interval 120
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring OSPF Route Summarization

In large scale OSPF networks, configuring route summarization can effectively reduce the size of routing table and free up system resources while maintaining system performance. In addition, if a link within the aggregated IP address range frequently goes up and down, the change will not be notified to the upstream devices. OSPF is a CPU intensive protocol especially in large deployments. Constant route flapping can impact the performance of a router significantly. Route summarization will shield all the upstream routers from constantly processing and updating routing information caused by route flapping.

Configuring ABR Route Summarization

The following commands can be used to configure OSPF route summarization.

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} range** <*prefix/mask*> [**advertise** <**true | false**> **| cost** <*cost*> **| substitute** <*prefix/mask*>]

set protocols ospf6 [vrf <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} range** <*prefix/mask*> [**advertise** <**true | false**> **| cost** <*cost*>]

Route summarization is configured on ABRs. Since ABRs share routing LSAs with other regions, if there are large number of destinations in an area, flooding all this information individually using separate LSA for each destination can easily overwhelm routers processing these LSAs. Instead, we can specify a range of routing subnets to be summarized or grouped into a single segment and shared with other regions. This can save both router processing cycles and also minimize the size of the routing table on routers receiving the summary LSAs.

The following commands configure route summarization in OSPF area 1.

```
admin@Xorplus# set protocols ospf area 1 range 10.42.0.0/16
admin@Xorplus# commit
```

Configuring ASBR Route Summarization

When the imported routes have the same routing prefix, you can aggregate these introduced routes and publish them as one aggregated route by using the ASBR route summarization. By configuring route summarization, you can reduce the routing information and the size of the routing table to improve the performance of the device.

The following commands can be used to configure ASBR route summarization.

set protocols ospf [vrf <*vrf-name*>] **summary-address** <*prefix/mask*> **[no-advertise | tag** <*tag-value*>**]**

set protocols ospf [vrf <*vrf-name*>**] aggregation timer** <*aggregation-timer*>

The following commands configure OSPF route summarization for ASBR.

```
admin@Xorplus# set protocols ospf summary-address 10.2.0.0/16 tag 2
admin@Xorplus# set protocols ospf aggregation timer 100
admin@Xorplus# commit
```

You can use the command **run show ospf summary-address** to show the configuration for display all configured summary routes with matching external LSA information.

```
admin@Xorplus# run show ospf summary-address
Summary-address     Metric-type     Metric     Tag       External_Rt_count
aggregation delay interval :100(in seconds)
10.2.0.0/16           E2              20        2        0
```

Basic OSPF Configuration Example

Open Shortest Path First (OSPF) is a widely used routing protocol based on the Dijkstra's Shortest Path First algorithm that determines the shortest path for packets to reach a destination. This is opposed to the older Routing Information Protocol (RIP) in which best path is based on the fewest number of “hops” to the destination, meaning that a path in which the packet would have to traverse the fewest number of routers is considered the best one. OSPF is an interior gateway protocol (IGP) intended for use in a single routing domain, or autonomous system (AS). It is a dynamic routing protocol that, like RIP, changes routing tables whenever the network topology changes. It determines the shortest path through a network based on the “cost” of the route, meaning it considers the amount of available bandwidth, delay and load on different network segments. This document describes an example of basic OSPF configuration for PICOS-based switches.

Fig.5-3 presents an example topology for configuring OSPF routing. There are two areas configured in this network, Router 1 has two interfaces both in area 1 whereas Router 2 and 3 have two interfaces each, with one interface each in area 0 and area1.

After OSPF is configured on the four routers, the routers will send LSAs to each and hence will have routes to all the subnets in the network. Router1 will have routes to all the connected subnets of Router2, Router3 and Router4. Similarly, all the other routers will have access to all the other subnets configured for OSPF. The detailed configuration of each router is shown below.

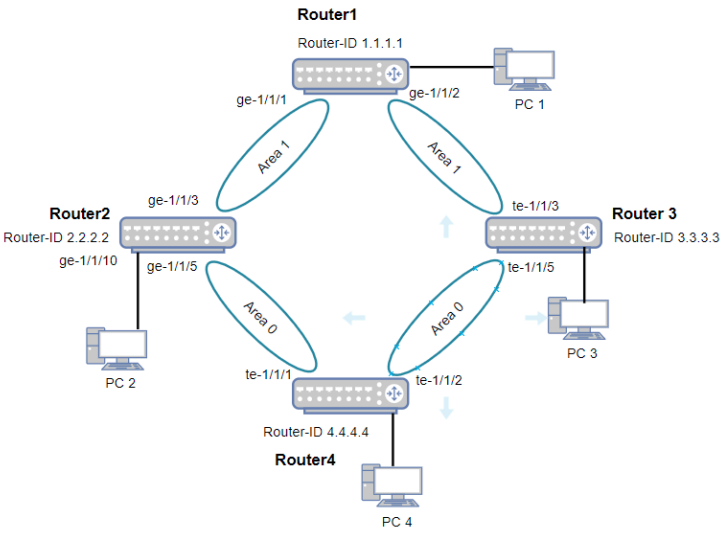


Figure 5-3 Basic OSPF Configuration

Configuring Router 1

Configure 2 VLAN interfaces for networks 10.1.1.0/24 and 20.1.1.0/24. There is only one area configured on Router 1, area 1 which include networks 10.1.1.0/24 and 20.1.1.0/24.

```
admin@router1# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@router1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@router1# set protocols ospf router-id 1.1.1.1
admin@router1# set protocols ospf network 10.1.1.0/24 area 1
admin@router1# set protocols ospf network 20.1.1.0/24 area 1
admin@router1# set protocols ospf network 1.1.1.1/32 area 1
admin@router1# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@router1# set l3-interface vlan-interface vlan10 address 10.1.1.1 prefix-length 24
admin@router1# set l3-interface vlan-interface vlan20 address 20.1.1.1 prefix-length 24
admin@router1# set vlans vlan-id 10 l3-interface "vlan10"
admin@router1# set vlans vlan-id 20 l3-interface "vlan20"
```

Configuring Route 2

On Router 2, we will configure the router ID as 1.1.1.1 and configure two VLAN interfaces. For 10.1.1.1.0/24 we will configure interface vlan10 in area 1 and for network 30.1.1.0/24 we will configure interface vlan30 in area 0.

```
admin@router2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 10
admin@router2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 30
admin@router2# set protocols ospf router-id 2.2.2.2
admin@router2# set protocols ospf network 10.1.1.0/24 area 1
admin@router2# set protocols ospf network 30.1.1.0/24 area 0
admin@router2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@router2# set l3-interface vlan-interface vlan10 address 10.1.1.2 prefix-length 24
```

```
admin@router2# set l3-interface vlan-interface vlan30 address 30.1.1.1 prefix-length 24
admin@router2# set vlans vlan-id 10 l3-interface "vlan10"
admin@router2# set vlans vlan-id 30 l3-interface "vlan30"
```

Configuring Router 3

On Router 3 we will configure the router ID as 3.3.3.3 and two VLAN interfaces. Interface vlan10 for network 10.1.1.0/24 is added to area 1 and VLAN interface vlan30 for network 30.1.1.0/24 is added to area 0.

```
admin@router3# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 20
admin@router3# set interface gigabit-ethernet te-1/1/3 auto-speeds 1000
admin@router3# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 40
admin@router3# set interface gigabit-ethernet te-1/1/5 auto-speeds 1000
admin@router3# set protocols spanning-tree enable false
admin@router3# set protocols ospf router-id 3.3.3.3
admin@router3# set protocols ospf network 20.1.1.0/24 area 1
admin@router3# set protocols ospf network 40.1.1.0/24 area 0
admin@router3# set l3-interface vlan-interface vlan20 address 20.1.1.2 prefix-length 24
admin@router3# set l3-interface vlan-interface vlan40 address 40.1.1.1 prefix-length 24
admin@router3# set vlans vlan-id 20 l3-interface "vlan20"
admin@router3# set vlans vlan-id 40 l3-interface "vlan40"
admin@router3# commit
Commit OK.
Save done.
```

Configuring Router 4

The router ID on Router 4 is configured as 4.4.4.4 and two VLAN interfaces both of which are in area 0. VLAN interface vlan30 for network 30.1.1.0/24 is in area 0 and VLAN interface vlan40 for network 40.1.1.0/24 also belonging to area 0.

```
admin@router4# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 30
admin@router4# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 40
admin@router4# set protocols ospf router-id 4.4.4.4
admin@router4# set protocols ospf network 30.1.1.0/24 area 0
admin@router4# set protocols ospf network 40.1.1.0/24 area 0
admin@router4# set protocols ospf network 4.4.4.4/32 area 0
admin@router4# set protocols ospf redistribute static
admin@router4# set l3-interface loopback lo address 4.4.4.4 prefix-length 32
admin@router4# set l3-interface vlan-interface vlan30 address 30.1.1.2 prefix-length 24
admin@router4# set l3-interface vlan-interface vlan40 address 40.1.1.2 prefix-length 24
admin@router4# set vlans vlan-id 40 l3-interface vlan40
admin@router4# set vlans vlan-id 30 l3-interface vlan30
Commit OK.
Save done.
```

Verifying the OSPF configuration

We can verify the OSPF configuration of a switch by checking its OSPF neighbors by running the command **run show ospf neighbor.**
Below is the command output on Router 1. As we can see Router 1 has established neighbor relationship with Router 2 (router ID 2.2.2.2) and Router 3 (router ID 3.3.3.3).

```
admin@router1# run show ospf neighbor
Neighbor ID     Pri State           Dead Time Address         Interface                       RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR           35.852s 10.1.1.2        vlan.2:10.1.1.1                     0     0     0
3.3.3.3           1 Full/DR           31.187s 20.1.1.2        vlan.3:20.1.1.1                     0     0     0
```

Now check the OSPF database on Router 1 by running the command **run show ospf database.**

```
admin@router1# run show ospf database
OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1528 0x8000001e 0xe83f 4
2.2.2.2         2.2.2.2         1548 0x8000000f 0xcd41 1
3.3.3.3         3.3.3.3         1534 0x8000000f 0x3cb4 1

                Net Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.2        2.2.2.2         1578 0x80000009 0x0e22
20.1.1.2        3.3.3.3         1524 0x80000009 0x9f7e

                Summary Link States (Area 0.0.0.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
4.4.4.4         2.2.2.2         1328 0x80000009 0xcb30 4.4.4.4/32
4.4.4.4         3.3.3.3         1254 0x80000009 0xad4a 4.4.4.4/32
30.1.1.0        2.2.2.2         1288 0x8000000a 0xe23f 30.1.1.0/24
30.1.1.0        3.3.3.3         1334 0x80000009 0x2be9 30.1.1.0/24
40.1.1.0        2.2.2.2         1378 0x80000009 0xc648 40.1.1.0/24
40.1.1.0        3.3.3.3         1244 0x80000009 0x44d0 40.1.1.0/24
```

To check the IPv4 route table on Router 1, run the command **run show route ipv4.**

```
admin@router1# run show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 00:28:55
O   1.1.1.1/32 [110/10] via 0.0.0.0, loopback onlink, weight 1, 00:28:54
C>* 1.1.1.1/32 is directly connected, loopback, 00:28:55
O>* 4.4.4.4/32 [110/30] via 10.1.1.2, vlan10, weight 1, 00:21:34
  *                     via 20.1.1.2, vlan20, weight 1, 00:21:34
```

```
O   10.1.1.0/24 [110/10] is directly connected, vlan10, weight 1, 00:27:02
C>* 10.1.1.0/24 is directly connected, vlan10, 00:27:46
C>* 10.10.51.0/24 is directly connected, eth0, 00:28:55
O   20.1.1.0/24 [110/10] is directly connected, vlan20, weight 1, 00:24:56
C>* 20.1.1.0/24 is directly connected, vlan20, 00:25:56
O>* 30.1.1.0/24 [110/20] via 10.1.1.2, vlan10, weight 1, 00:21:37
O>* 40.1.1.0/24 [110/20] via 20.1.1.2, vlan20, weight 1, 00:22:26
```

OSPF Area Type Configuration Example: NSSA, Stub and Standard Areas

In OSPF terminology, a stub is an area in which external routes are not advertised. To reach external networks, a default summary route 0.0.0.0 is installed in the stub area to achieve connectivity with other areas. In the OSPF not-so-stubby-area (NSSA), the restriction on advertising external routes in the NSSA area is removed but in a limited fashion.

Configuration Example

Figure 5-4 depicts a sample OSPF topology with three different types of areas, the Standard, NSSA and the stub areas.

The configuration of OSPF NSSA and stub areas is shown in Fig. 5-4. Router 2 connects to the backbone area (area 0) through Router 4. This area between Switch 4 and Switch 3 is configured as the not-so-stubby-area (NSSA). Similarly, Router 1 connects with the backbone area through Router 2. Both Router 4 and Router 2 have one interface each in area 0. Router 3 will receive routes for network 10.10.4.0/24, 10.10.3.0/24, 10.10.2.0/24 and 10.10.1.0/24. Similarly, Router 1 will receive routes from network 10.10.3.0/24, 10.10.4.0/24, 10.10.5.0/24 and 10.10.6.0/24.

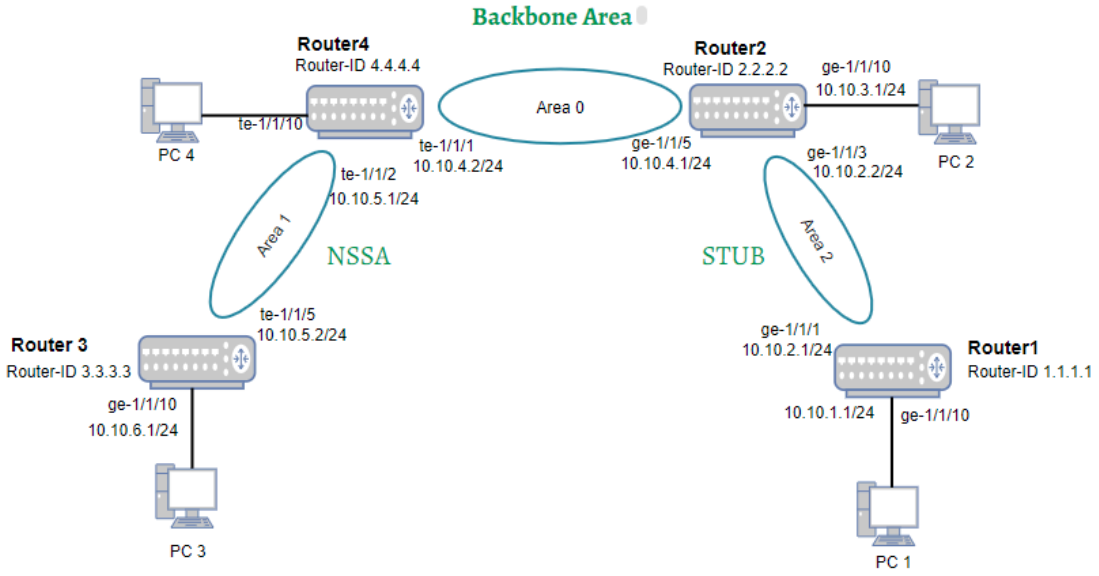


Figure 5-4. OSPF NSSA and Stub area configurations.

Configuring Router 1

On Router 1, we will configure one VLAN interface for network 10.10.2.1/24. Also we will configure OSPF area 0.0.0.2 and include network 10.10.2.1/24 in area 2.

```
admin@router1# set vlans vlan-id 10 l3-interface vlan10
admin@router1# set vlans vlan-id 20 l3-interface vlan20
admin@router1# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@router1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@router1# set protocols ospf router-id 1.1.1.1
admin@router1# set protocols ospf network 10.10.2.0/24 area 0.0.0.2
admin@router1# set protocols ospf network 1.1.1.1/32 area 0.0.0.2
admin@router1# set protocols ospf area 2 area-type stub
admin@router1# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@router1# set l3-interface vlan-interface vlan10 address 10.10.2.1 prefix-length 24
admin@router1# set l3-interface vlan-interface vlan20 address 10.10.1.1 prefix-length 24
Commit OK.
Save done.
admin@router1#
```

Configuring Router 2

Router 2 has to VLAN interfaces, one in area 0.0.0.2 and another in area 0.0.0.0. We will configure these interfaces for network 10.10.2.0/24 and 10.10.4.0/24 in the configuration shown below.

```
admin@router2# set vlans vlan-id 30 l3-interface "vlan30"
admin@router2# set vlans vlan-id 40 l3-interface "vlan40"
admin@router2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@router2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 40
admin@router2# set protocols ospf router-id 2.2.2.2
```

```
admin@router2# set protocols ospf network 10.10.2.0/24 area 0.0.0.2
admin@router2# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router2# set protocols ospf area 0.0.0.2 area-type stub
admin@router2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@router2# set l3-interface vlan-interface vlan30 address 10.10.2.2 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan40 address 10.10.4.1 prefix-length 24
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Router 3

On Router 3 we will configure one OSPF interface in area 0.0.0.1.

```
admin@router3# set vlans vlan-id 50 l3-interface vlan50
admin@router3# set l3-interface vlan-interface vlan50 address 10.10.5.2 prefix-length 24
admin@router3# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 50
admin@router3# set interface gigabit-ethernet te-1/1/5 auto-speeds 1000
admin@router3# set protocols spanning-tree enable false
admin@router3# set protocols ospf router-id 3.3.3.3
admin@router3# set protocols ospf network 10.10.5.0/24 area 0.0.0.1
admin@router3# set protocols ospf area 0.0.0.1 area-type nssa
admin@router3# commit
Commit OK.
Save done.
```

Configuring Router 4

On Router 4 we will configure two network interfaces one each in area 0.0.0.0 and 0.0.0.1. Router 4 connects with Router 3 in area 0.0.0.1 and Router 2 in area 0.0.0.0.

```
admin@router4# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 40
admin@router4# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 50
admin@router4# set protocols ospf router-id 4.4.4.4
admin@router4# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router4# set protocols ospf network 10.10.5.0/24 area 0.0.0.1
admin@router4# set protocols ospf area 0.0.0.1 area-type nssa
admin@router4# set protocols ospf network 4.4.4.4/32 area 0
admin@router4# set protocols ospf redistribute static
admin@router4# set l3-interface loopback lo address 4.4.4.4 prefix-length 32
admin@router4# set l3-interface vlan-interface vlan40 address 10.10.4.2 prefix-length 24
admin@router4# set l3-interface vlan-interface vlan50 address 10.10.5.1 prefix-length 24
admin@router4# set vlans vlan-id 40 l3-interface "vlan40"
admin@router4# set vlans vlan-id 50 l3-interface "vlan50"
Commit OK.
Save done.
```

Verify Routing Table

The routing table on Router 1 is displayed below.

```
admin@router1> show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O   0.0.0.0/0 [110/11] via 10.10.2.2, vlan10, weight 1, 00:08:11
K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 02:35:35
O   1.1.1.1/32 [110/0] is directly connected, lo, weight 1, 02:16:35
C>* 1.1.1.1/32 is directly connected, lo, 02:16:35
O>* 4.4.4.4/32 [110/20] via 10.10.2.2, vlan10, weight 1, 00:06:55
O   10.10.2.0/24 [110/10] is directly connected, vlan10, weight 1, 00:46:21
C>* 10.10.2.0/24 is directly connected, vlan10, 00:47:01
O>* 10.10.4.0/24 [110/20] via 10.10.2.2, vlan10, weight 1, 00:07:05
O>* 10.10.5.0/24 [110/30] via 10.10.2.2, vlan10, weight 1, 00:02:25
```

The routing table on Router 3 is displayed below.

```
admin@router3> show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O   0.0.0.0/0 [110/11] via 10.10.5.1, vlan50, weight 1, 00:16:09
O>* 1.1.1.1/32 [110/30] via 10.10.5.1, vlan50, weight 1, 00:16:09
O>* 4.4.4.4/32 [110/10] via 10.10.5.1, vlan50, weight 1, 00:16:09
O>* 10.10.2.0/24 [110/30] via 10.10.5.1, vlan50, weight 1, 00:16:09
O>* 10.10.4.0/24 [110/20] via 10.10.5.1, vlan50, weight 1, 00:16:09
O   10.10.5.0/24 [110/10] is directly connected, vlan50, weight 1, 00:21:59
C>* 10.10.5.0/24 is directly connected, vlan50, 00:21:59
```

OSPF Stub and NSSA Areas with no-summary

By default, external routes and inter-area routes will be injected into stub or NSSAs areas in the same OSPF domain in the absence of effective route summarization. This can overwhelm a node particularly in large OSPF routing domains. Changing an area from stub to a *totally-stubby* area solves this issue. To change an area from stub to a totally-stubby-area, user can apply the command **set protocols ospf area 0.0.0.1 no-summary** from the PiCOS configuration mode.

In Figure 5-5 below, Router 2 is an ABR, to reduce the number of routes on Router 1 in area 0.0.0.2, we will configure area 0.0.0.2 on Router 2 as a totally stubby area.

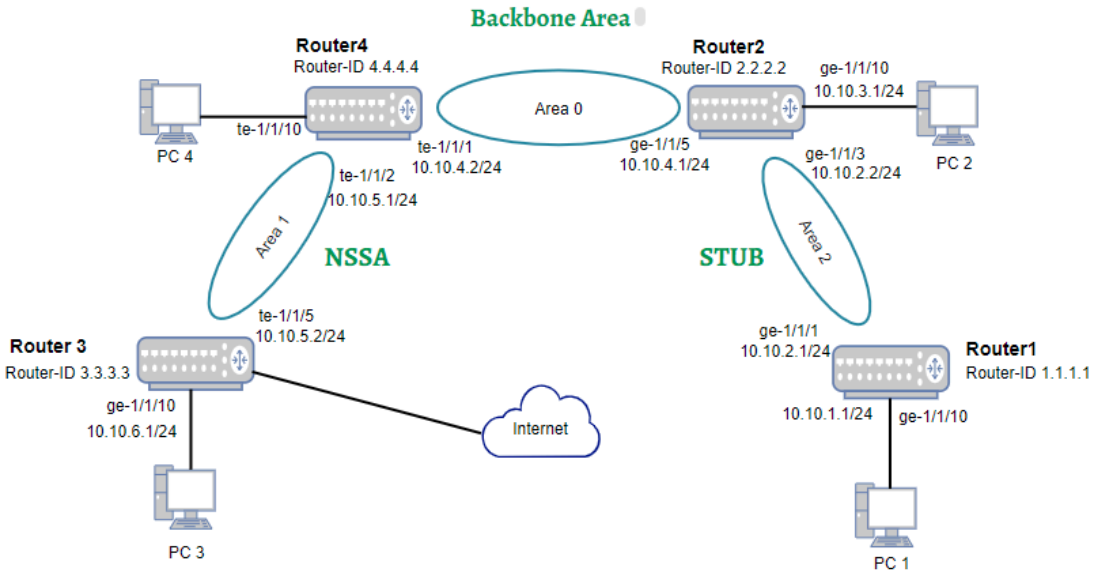


Figure 5-5. OSPF Stub area/NSSA summary: area 1.1.1.1 should be a stub area or an NSSA

Configuring Router 2

```
admin@router2# set vlans vlan-id 30 l3-interface "vlan30"
admin@router2# set vlans vlan-id 40 l3-interface "vlan40"
admin@router2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@router2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 40
admin@router2# set l3-interface vlan-interface vlan30 address 10.10.2.2 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan40 address 10.10.4.1 prefix-length 24
admin@router2# set protocols ospf router-id 2.2.2.2
admin@router2# set protocols ospf area 0.0.0.2 area-type "stub"
admin@router2# set protocols ospf area 0.0.0.2 no-summary
admin@router2# set protocols ospf network 10.10.2.0/24 area 0.0.0.2
admin@router2# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router2# set l3-interface loopback lo address 2.2.2.2 32 prefix-length 32
Commit OK.
Save Done.
admin@router2#
```

Similarly, on Router4, we will run the same command to stop injecting summaries in NSSA area 0.0.0.1.

Configuring Router 4

```
admin@router4# set vlans vlan-id 40 l3-interface "vlan40"
admin@router4# set vlans vlan-id 50 l3-interface "vlan50"
admin@router4# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 40
admin@router4# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 50
admin@router4# set l3-interface vlan-interface vlan40 address 10.10.4.2 prefix-length 24
admin@router4# set l3-interface vlan-interface vlan50 address 10.10.5.1 prefix-length 24
admin@router4# set protocols ospf router-id 4.4.4.4
admin@router4# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router4# set protocols ospf network 10.10.5.0/24 area 0.0.0.1
admin@router4# set protocols ospf area 0.0.0.1 area-type nssa
admin@router4# set protocols ospf area 0.0.0.1 no-summary
admin@router4# set protocols ospf network 4.4.4.4/32 area 0
admin@router4# set protocols ospf redistribute static
admin@router4# set l3-interface loopback lo address 4.4.4.4 prefix-length 32
Commit OK.
Save done.
```

OSPF Area Range Configuration Guide

OSPF should aggregate route entries from the backbone area into a non-backbone area or from a non-backbone area into the backbone area. Route aggregation works only on the ABR.

To disable injecting routes into an area from an ABR manually, the user can apply the prefix lists in *inbound* or *outbound* directions to control the dissemination of routes into and out of OSPF areas. The command used to control route dissemination is **set protocols ospf area in filter-list prefix**. The keyword **in** indicated routes advertised into an area. Whereas **out** indicates routes going out of the area. Its important to note that the user must configure the prefix list before applying it through the **set protocols ospf area in filter-list prefix** command. The command to create the prefix list is **set routing prefix-list.**

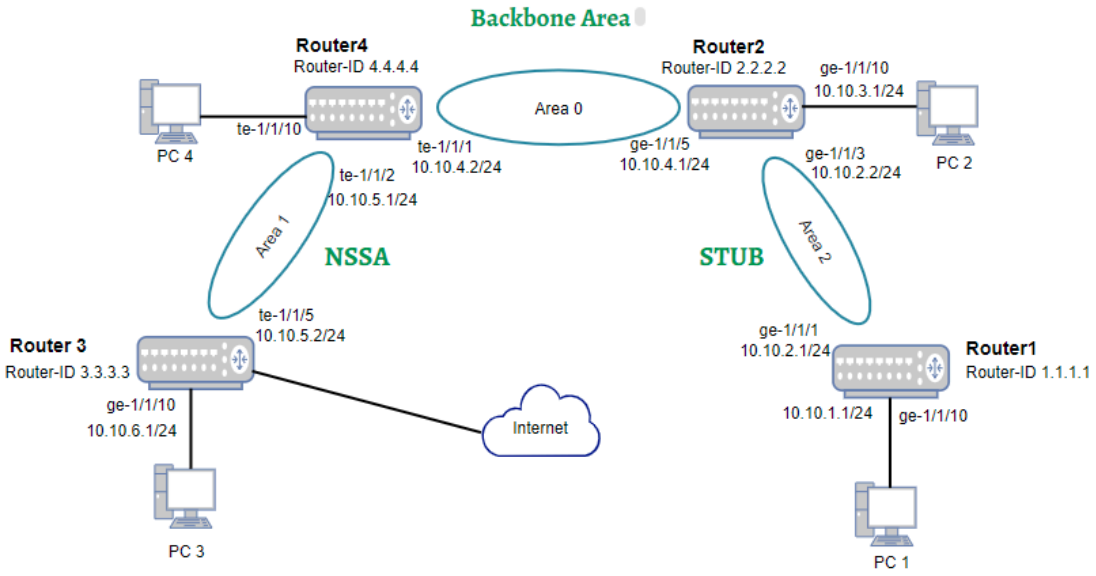


Figure 5-6. OSPF area range configuration.

Figure 5-6 shows a sample OSPF topology with three different areas configured. In this example we will focus on the configuration on Router 2 to see how it affects the routing table on Router 1 which is in area 0.0.0.2. First we will see the configuration on Router 2.

Configuring Router 2

```
admin@router2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@router2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 40
admin@router2# set protocols lldp enable true
admin@router2# set protocols ospf router-id 2.2.2.2
admin@router2# set protocols ospf area 0.0.0.2 area-type "stub"
admin@router2# set protocols ospf area 0.0.0.1 in filter-list
admin@router2# set protocols ospf network 10.10.2.0/24 area 0.0.0.2
admin@router2# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router2# set system hostname "router2"
admin@router2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@router2# set l3-interface vlan-interface vlan30 address 10.10.2.2 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan40 address 10.10.4.1 prefix-length 24
admin@router2# set vlans vlan-id 30 l3-interface "vlan30"
admin@router2# set vlans vlan-id 40 l3-interface "vlan40"
```

Check the Routing Table on Router 1

If we check the routing table on Router 1, we can see prefix 10.10.5.0 is in the routing table advertised through OSPF.

```
admin@router1> show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O   0.0.0.0/0 [110/11] via 10.10.2.2, vlan10, weight 1, 04:01:47
O   1.1.1.1/32 [110/0] is directly connected, lo, weight 1, 04:03:37
C>* 1.1.1.1/32 is directly connected, lo, 04:03:37
```

```
O>* 4.4.4.4/32 [110/20] via 10.10.2.2, vlan10, weight 1, 00:00:02
O   10.10.2.0/24 [110/10] is directly connected, vlan10, weight 1, 04:02:37
C>* 10.10.2.0/24 is directly connected, vlan10, 04:02:37
O>* 10.10.4.0/24 [110/20] via 10.10.2.2, vlan10, weight 1, 00:00:02
O>* 10.10.5.0/24 [110/30] via 10.10.2.2, vlan10, weight 1, 00:00:02
```

Now we will add the commands **set protocols ospf area 0.0.0.2 in filter-list prefix list1** and **set routing prefix-list IPv4 list1 deny prefix 10.10.5.0/24** to Router 2.

```
admin@router2# set routing prefix-list IPv4 list1 deny prefix 10.10.5.0/24
admin@router2# set protocols ospf area 0.0.0.2 in filter-list prefix "list1"
Commit OK.
Save Done.
admin@router2#
```

Now if we check the routing table on Router 1 again, we see the prefix 10.10.5.0/24 has disappeared from the routing table.

```
admin@router1> show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O   0.0.0.0/0 [110/11] via 10.10.2.2, vlan10, weight 1, 04:54:16
K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 04:56:35
O   1.1.1.1/32 [110/0] is directly connected, lo, weight 1, 04:56:06
C>* 1.1.1.1/32 is directly connected, lo, 04:56:06
O   10.10.2.0/24 [110/10] is directly connected, vlan10, weight 1, 04:55:06
C>* 10.10.2.0/24 is directly connected, vlan10, 04:55:06
```

OSPF Route Redistribution and Route Maps

OSPF has the ability to redistribute routes of other routing protocols in the routing table into OSPF. In OSPF terminology, routes from other routing protocols are known as external routes and they can be redistributed into OSPF as Type-5 LSAs.

When redistributing external routes, we can specify filters to control which type of routes are redistributed into OSPF otherwise it has the potential to overwhelm the OSPF process especially in large networks. It also gives the administrator the ability to stop advertising unnecessary routes through OSPF. Filtering of routes for redistribution is achieved by route maps. To create a route map, we can run the command **set routing route-map <***map-name***>**.

In the following section we will demonstrate route redistribution and the use of route map in a sample topology shown in Figure 1.

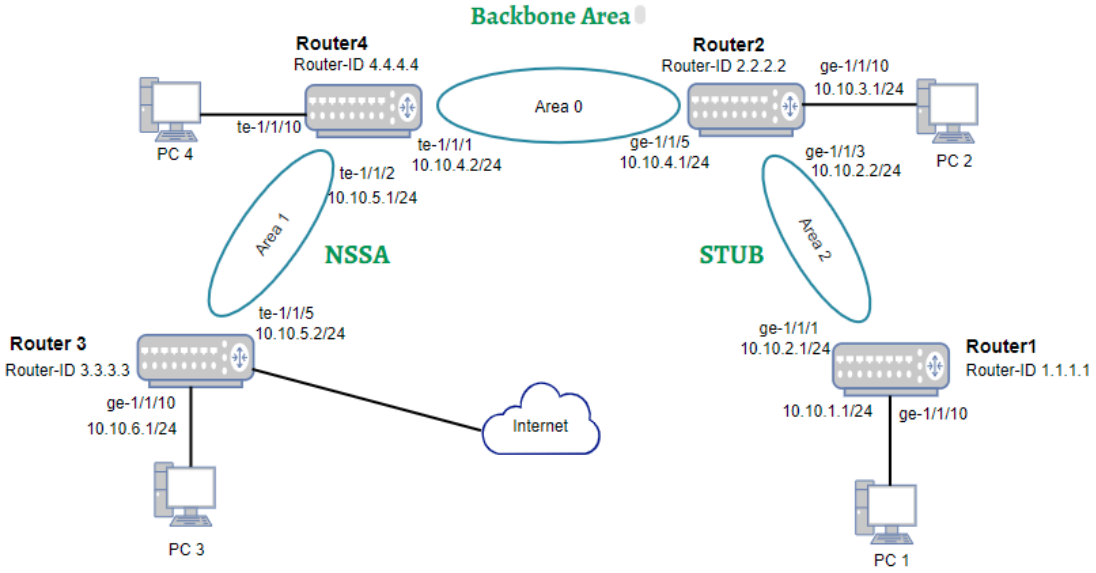


Figure 1 OSPF Route Redistribution and Route Maps

Configuration on Router 2

On Router 2, we have the following basic OSPF configuration.

```
admin@router2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@router2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 40
admin@router2# set protocols ospf router-id 2.2.2.2
admin@router2# set protocols ospf area 0.0.0.2 area-type stub
admin@router2# set protocols ospf network 10.10.2.0/24 area 0.0.0.2
admin@router2# set protocols ospf network 10.10.4.0/24 area 0.0.0.0
admin@router2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@router2# set l3-interface vlan-interface vlan30 address 10.10.2.2 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan40 address 10.10.4.1 prefix-length 24
admin@router2# set vlans vlan-id 30 l3-interface vlan30
admin@router2# set vlans vlan-id 40 l3-interface vlan40
Commit OK.
Save done.
admin@router2#
```

If we wish to redistribute external routes through OSPF, we can configure the **set protocols ospf redistribute** command. And then configure a route map to control which type or specific prefixes are allowed to be redistributed through OSPF. The configuration shown below permits the redistribution of prefix 2.2.2.3/32 through OSPF.

```
admin@router2# set routing prefix-list IPv4 list2 permit prefix 2.2.2.3/32
admin@router2# set routing route-map map2 order 1 matching-policy "permit"
admin@router2# set routing route-map map2 order 1 match ip address prefix-list "list2"
admin@router2# set protocols ospf redistribute connected route-map "map2"
```

The configuration above first creates a prefix list *list2,* which permits prefix 2.2.2.3/32. Then create a route map *map2* with matching policy of permit. The match IP for map2 is set to *list2.* Finally, the command **set protocols ospf redistribute connected route-map map2** applies the configuration to Router 2. We can confirm that the prefix is advertised to Router 4 by checking the routing table on Router 4.

```
admin@router4> show route ipv4
Possible completions:
  <ip-address>                   An IPv4/IPv6 address or prefix length
  ipv4                           IPv4
admin@router4> show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 04:05:50
O>* 2.2.2.3/32 [110/20] via 10.10.4.1, vlan40, weight 1, 04:03:30        <-----OSPF Redistributed Prefix
O   4.4.4.4/32 [110/0] is directly connected, lo, weight 1, 04:05:23
C>* 4.4.4.4/32 is directly connected, lo, 04:05:23
O>* 10.10.2.0/24 [110/20] via 10.10.4.1, vlan40, weight 1, 01:55:32
O   10.10.4.0/24 [110/10] is directly connected, vlan40, weight 1, 04:04:21
C>* 10.10.4.0/24 is directly connected, vlan40, 04:04:21
O   10.10.5.0/24 [110/10] is directly connected, vlan50, weight 1, 04:04:02
C>* 10.10.5.0/24 is directly connected, vlan50, 04:04:21
```

The OSPF redistribute command can redistribute the following types of external routes.

- **BGP Routes**
- **Connected Routes**
- **Kernel Routes**
- **Static Routes**
- **Table**

We can also specify the OSPF metric for these routes, for example run the command **set protocols ospf redistribute static metric** to specify the metric for the redistributed static routes.

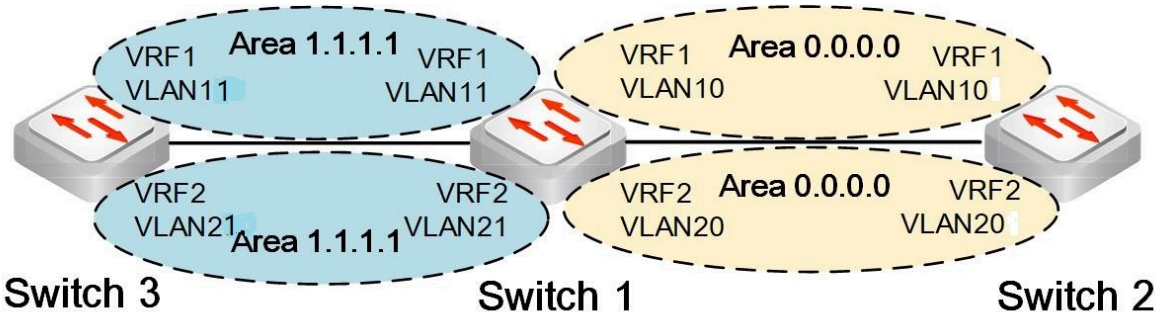
Example for Configuring OSPF with Different VRFs

- Networking Requirements
  - Basic Deployment
  - Networking Address Planning
- Procedure
  - Switch1
  - Switch2
  - Switch3
- Verify the Configuration

Networking Requirements

As shown in **Figure 1**, by configuring OSPF routing protocol on switch 1, switch 2 and switch 3, the three devices can exchange routing information with each other. We will implement the VRF function on Switch 1, Switch 2 and Switch 3 to segregate the users' routing spaces of different Tenants. We will create two VRFs on each device and run OSPF in these VRFs.

Figure1. User Configuration Topology of OSPF with Different VRFs



Basic Deployment

Figure 1 shows the user configuration topology of OSPF with different VRFs. Follow the configuration roadmap below to complete the configuration.

- Configure IP addresses and VLANs for the VLAN interfaces on switches to establish communication within the network segments.
- Configure basic OSPF functions on each switch. Configure Switch 1 as the ABR to divide the OSPF network into two areas (Area: 0.0.0.0 and Area: 1.1.1.1), so that the entire OSPF network can be extended using the area where Switch 1 and Switch 2 are located as the backbone area.
- In order to make different tenants have different routing space, configure two VRFs on each of the three switches.

Networking Address Planning

The networking IP address planning is shown in the following table.

Switch	Physical Interface	VRF and VLAN Interface	OSPF Configurations
Switch1	Te-1/1/1	vrf1 VLANIF11: 11.251.201.2	Area: 1.1.1.1 Router ID: 1.1.1.1
		vrf2 VLANIF 21: 21.251.201.2	Area: 1.1.1.1 Router ID: 1.1.1.1
	Te-1/1/2	vrf1 VLANIF 10: 10.251.201.2	Area: 0.0.0.0 Router ID: 1.1.1.1
		vrf2 VLANIF 20: 20.251.201.2	Area: 0.0.0.0 Router ID: 1.1.1.1
Switch2	Te-1/1/5	vrf1 VLANIF 10: 101.251.201.3	Area: 0.0.0.0 Router ID: 2.2.2.2
		vrf2 VLANIF 20: 201.251.201.3	Area: 0.0.0.0 Router ID: 2.2.2.2
Switch3	Te-1/1/5	vrf1 VLANIF 11: 100.251.201.3	Area: 1.1.1.1 Router ID: 3.3.3.3
		vrf2 VLANIF 21: 200.251.201.3	Area: 1.1.1.1 Router ID: 3.3.3.3

Procedure

Configure Switch 1, Switch 2 and Switch 3 according to the networking requirements described above.

Switch1

Step1 Configure the VLANs and VLAN interfaces.

```
admin@switch1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@switch1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 11
admin@switch1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 21
admin@switch1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 10
admin@switch1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@switch1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 10
admin@switch1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 20
admin@switch1# set l3-interface loopback vrf1 address 1.1.1.1 prefix-length 32
admin@switch1# set l3-interface vlan-interface vlan10 address 10.251.201.2 prefix-length 24
admin@switch1# set l3-interface vlan-interface vlan20 address 20.251.201.2 prefix-length 24
admin@switch1# set l3-interface vlan-interface vlan11 address 11.251.201.2 prefix-length 24
admin@switch1# set l3-interface vlan-interface vlan21 address 21.251.201.2 prefix-length 24
admin@switch1# set vlans vlan-id 10 l3-interface vlan10
admin@switch1# set vlans vlan-id 11 l3-interface vlan11
admin@switch1# set vlans vlan-id 20 l3-interface vlan20
admin@switch1# set vlans vlan-id 21 l3-interface vlan21
```

Step2 Configure VRF.

a. Enable IP routing function before using VRF function and configure the system hostname.

```
admin@switch1# set ip routing enable true
admin@switch1# set system hostname switch1
```

b. Create VRFs.

```
admin@switch1# set ip vrf vrf1 description orange
admin@switch1# set ip vrf vrf2 description purple
```

c. Bind the Layer 3 VLAN interface to the VRF.

```
admin@switch1# set l3-interface vlan-interface vlan10 vrf vrf1
admin@switch1# set l3-interface vlan-interface vlan20 vrf vrf2
admin@switch1# set l3-interface vlan-interface vlan11 vrf vrf1
admin@switch1# set l3-interface vlan-interface vlan21 vrf vrf2
```

Step3 Configure basic OSPF functions.

```
admin@switch1# set protocols ospf vrf vrf1 router-id 1.1.1.1
admin@switch1# set protocols ospf vrf vrf1 network 10.251.201.0/24 area 0.0.0.0
admin@switch1# set protocols ospf vrf vrf1 network 11.251.201.0/24 area 1.1.1.1
admin@switch1# set protocols ospf vrf vrf2 router-id 1.1.1.1
admin@switch1# set protocols ospf vrf vrf2 network 20.251.201.0/24 area 0.0.0.0
admin@switch1# set protocols ospf vrf vrf2 network 21.251.201.0/24 area 1.1.1.1
```

Step4 Commit the configuration.

```
admin@Switch1# commit
```

Switch2

Step1 Configure the VLANs and VLAN interfaces.

```
admin@switch2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode "trunk"
admin@switch2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 10
admin@switch2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 20
admin@switch2# set vlans vlan-id 10 l3-interface "vlan10"
admin@switch2# set vlans vlan-id 20 l3-interface "vlan20"
admin@switch2# set l3-interface vlan-interface vlan20 address 20.251.201.3 prefix-length 24
admin@switch2# set l3-interface vlan-interface vlan10 address 10.251.201.3 prefix-length 24
```

Step2 Configure VRF.

a. Enable IP routing function before using VRF function and set the system hostname.

```
admin@switch2# set ip routing enable true
admin@switch2# set system hostname "switch2"
```

b. Create VRFs.

```
admin@switch2# set ip vrf vrf1 description orange
admin@switch2# set ip vrf vrf2 description purple
```

c. Bind the Layer 3 VLAN interface to the VRF.

```
admin@switch2# set l3-interface vlan-interface vlan10 vrf "vrf1"
admin@switch2# set l3-interface vlan-interface vlan20 vrf "vrf2"
```

Step3 Configure basic OSPF functions.

```
admin@switch2# set protocols ospf vrf vrf1 router-id 2.2.2.2
admin@switch2# set protocols ospf vrf vrf1 network 10.251.201.0/24 area 0.0.0.0
admin@switch2# set protocols ospf vrf vrf2 router-id 2.2.2.2
admin@switch2# set protocols ospf vrf vrf2 network 20.251.201.0/24 area 0.0.0.0
```

Step4 Commit the configuration.

```
admin@switch2# commit
```

Switch3

Step1 Configure the VLANs and VLAN interfaces.

```
admin@switch3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode "trunk"
admin@switch3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 11
admin@switch3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 21
admin@switch3# set vlans vlan-id 11 l3-interface "vlan11"
admin@switch3# set vlans vlan-id 21 l3-interface "vlan21"
admin@switch3# set l3-interface vlan-interface vlan11 address 11.251.201.4 prefix-length 24
admin@switch3# set l3-interface vlan-interface vlan21 address 21.251.201.4 prefix-length 24
```

Step2 Configure VRF.

a. Enable IP routing function before using VRF function.

```
admin@switch3# set ip routing enable true
admin@switch3# set system hostname "switch3"
```

b. Create VRFs.

```
admin@Switch3# set ip vrf vrf1 description orange
admin@Switch3# set ip vrf vrf2 description purple
```

c. Bind the Layer 3 VLAN interface to the VRF.

```
admin@switch3# set l3-interface vlan-interface vlan11 vrf "vrf1"
admin@switch3# set l3-interface vlan-interface vlan21 vrf "vrf2"
```

Step3 Configure basic OSPF functions.

```
admin@switch3# set protocols ospf vrf vrf1 router-id 3.3.3.3
admin@switch3# set protocols ospf vrf vrf1 network 11.251.201.0/24 area 1.1.1.1
admin@switch3# set protocols ospf vrf vrf2 router-id 3.3.3.3
admin@switch3# set protocols ospf vrf vrf2 network 21.251.201.0/24 area 1.1.1.1
```

Step4 Commit the configuration.

```
admin@switch3# commit
```

Verify the Configuration

- You can use the run show vrf command to view the binding information between VRFs and the Layer 3 VLAN interfaces.

```
admin@switch1# run show vrf
Vrf          Description       Interfaces
----------   ---------------   ------------------------
vrf1         orange            vlan10,vlan11
vrf2         purple            vlan20,vlan21


admin@switch2# run show vrf
Vrf          Description       Interfaces
----------   ---------------   ------------------------
vrf1         orange            vlan10
vrf2         purple            vlan20
```

- You can use the **run show route vrf** command to check the routing table information of the specific VRF.

```
admin@switch3# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 05:25:24
O>* 10.251.201.0/24 [110/20] via 11.251.201.2, vlan11, weight 1, 01:34:21
O   11.251.201.0/24 [110/10] is directly connected, vlan11, weight 1, 02:48:16
C>* 11.251.201.0/24 is directly connected, vlan11, 02:48:31



show ipv6 route vrf vrf1
=========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
C>* fe80::/64 is directly connected, vlan11, 02:48:29
```

- To the check OSPF neighbor, run the command **run show ospf vrf neighbor.**

```
root@switch1# run show ospf vrf vrf1 neighbor
VRF Name: vrf1

Neighbor ID     Pri State           Dead Time Address         Interface                        RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR           36.055s 10.251.201.3    vlan10:10.251.201.2                  0     0     0
3.3.3.3           1 Full/Backup       36.899s 11.251.201.4    vlan11:11.251.201.2                  0     0     0
```

OSPFv3 Configuration Guide

We will demonstrate a sample OSPFv3 configuration in this guide. The topology consists of two switches, Switch1 and Switch2.

Both OSPF version 2 and 3 can be configured primarily using two different methods. Either we directly specify the interfaces and enable OSPFv3 on them or we enable OSPFv3 on a network prefix. If we use a network prefix to enable OSPF then all the interfaces who share the same network prefix become part of the OSPF network and OSPFv3 tries to create adjacencies with peers on these interfaces. These interfaces are advertised to peers using Type-1 Router LSAs. In this example we will use interface names to enable OSPFv3.

Figure 1. below depicts our basic OSPFv3 sample topology.

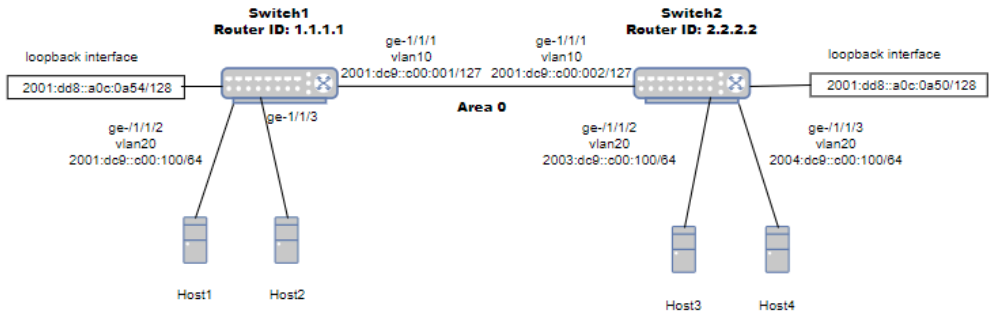


Figure 1. OSPFv3 Sample Configuration

Switch Configuration

Below is the switch configuration for the two switches, Switch1 and Switch2.

Switch1 Configuration

Interface ge-1/1/1 connects with Switch1. Interface ge-1/1/2 and ge-1/1/3 connects with hosts. The host-connecting interfaces will be put in passive mode. Which means that these interfaces will be advertised to Switch2 but OSPFv3 will not attempt to form any adjacencies on these two interfaces.

```
admin@Switch1# set vlans vlan-id 10
admin@Switch1# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@Switch1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@Switch1# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@Switch1# set vlans vlan-id 10 l3-interface vlan10
admin@Switch1# set l3-interface loopback lo address 2001:dd8::a0c:0a54 prefix-length 128
admin@Switch1# set l3-interface vlan-interface vlan10 address 2001:dc9::c00:001 prefix-length 127
admin@Switch1# set l3-interface vlan-interface vlan20 address 2001:dc9::c00:100 prefix-length 64
admin@Switch1# set l3-interface vlan-interface vlan30 address 2002:dc9::c00:100 prefix-length 64
admin@Switch1# set protocols ospf6 router-id 1.1.1.1
admin@Switch1# set protocols ospf6 interface lo area 0.0.0.0
admin@Switch1# set protocols ospf6 interface vlan10 area 0.0.0.0
admin@Switch1# set protocols ospf6 interface vlan20 area 0.0.0.0
admin@Switch1# set protocols ospf6 interface vlan30 area 0.0.0.0
admin@Switch1# set protocols ospf6 interface vlan20 passive
admin@Switch1# set protocols ospf6 interface vlan30 passive
admin@Switch1# set protocols ospf6 interface vlan10 network point-to-point
admin@Switch1# commit
```

Switch2 Configuration

The Switch2 configuration is almost identical to Switch1, the host-connecting interfaces are put in passive mode.

```
admin@Switch2# set vlans vlan-id 10
admin@Switch2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@Switch2# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@Switch2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 30
admin@Switch2# set vlans vlan-id 10 l3-interface vlan10
```

```
admin@Switch2# set l3-interface loopback lo address 2001:dd8::a0c:0a50 prefix-length 128
admin@Switch2# set l3-interface vlan-interface vlan10 address 2001:dc9::c00:002 prefix-length 127
admin@Switch2# set l3-interface vlan-interface vlan20 address 2003:dc9::c00:100 prefix-length 64
admin@Switch2# set l3-interface vlan-interface vlan30 address 2004:dc9::c00:100 prefix-length 64
admin@Switch2# set protocols ospf6 router-id 2.2.2.2
admin@Switch2# set protocols ospf6 interface lo area 0.0.0.0
admin@Switch2# set protocols ospf6 interface vlan10 area 0.0.0.0
admin@Switch2# set protocols ospf6 interface vlan20 area 0.0.0.0
admin@Switch2# set protocols ospf6 interface vlan30 area 0.0.0.0
admin@Switch2# set protocols ospf6 interface vlan20 passive
admin@Switch2# set protocols ospf6 interface vlan30 passive
admin@Switch2# set protocols ospf6 interface vlan10 network point-to-point
admin@Switch2# commit
```

Optional OSPFv3 Parameters

Hello Interval

To set the OSPFv3 interface hello interval to 5 seconds, run the following set command.

```
admin@Switch1# set protocols ospf6 interface vlan10 hello-interval 5
admin@Switch1# commit
```

Dead Interval

To set the OSPFv3 interface dead interval to 10 seconds, run the following set command.

```
admin@Switch1# set protocols ospf6 interface vlan10 dead-interval 10
admin@Switch1# commit
```

Priority

To set the OSPFv3 interface priority value to 5, run the below set command.

```
admin@Switch1# set protocols ospf6 interface vlan10 priority 5
admin@Switch1# commit
```

SPF Timers

To set the SPF initial delay to 1000ms, run the command below.

```
admin@Switch1# set protocols ospf6 timers throttle spf delay 1000
admin@Switch1# commit
```

To set the SPF initial hold-time to 2000ms, run the command below.

```
admin@Switch1# set protocols ospf6 timers throttle spf initial-holdtime 2000
admin@Switch1# commit
```

To set the SPF maximum hold-time to 10000ms, run the command below.

```
admin@Switch1# set protocols ospf6 timers throttle spf maximum-holdtime 10000
admin@Switch1# commit
```

OSPF Multi-Instance Support

> **NOTEs**:
>
> OSPF multi-instance is not supported in PICOS version 4.4.5.

OSPFv2 supports multiple instances of OSPF to run simultaneously on the device. Each instance is identified by an Instance ID which is a non-zero positive integer and must be provided when creating an instance.

Limitations of Multi-Instance OSPF

Multi-Instance OSPF can not coexist with single instance OSPF. If the user wants to configure multi-instance OSPF on a device which already has the single instance version of OSPF running then the user must first remove all the configuration related to single instance OSPF before configuring multi-instance OSPF.

Multiple instances of OSPFv2 can only be created in the default VRF. Multiple instances of OSPFv2 in the user defined (non-default) VRFs are not supported.

There are a maximum of 8 instances of OSPF allowed on a device.

The OSPF feature of enabling OSPF using the network command is not allowed under the multi-instance OSPF. Only by specifying a specific interface can the user enable OSPF on network interfaces.

Basic OSPF Multi-Instance Configuration

First of all we need to enable multi-instance OSPF on the device, run the command below to achieve this.

```
admin@Xorplus# set protocols ospf multi-instance disable false
admin@Xorplus# commit
```

To create an OSPF instance and configure the router ID, run the command below.

```
admin@Xorplus# set protocols ospf instance-id 5 router-id 1.1.1.1
admin@Xorplus# commit
```

Specify the backbone area for this instance and choose area-type as stub.

```
admin@Xorplus# set protocols ospf instance-id 5 area 0.0.0.0 area-type stub
admin@Xorplus# commit
```

Add a VLAN interface *vlan200* to the backbone area for instance ID 5. This command enables OSPF on the interface.

```
admin@Xorplus# set protocols ospf instance-id 5 interface vlan200 area 0.0.0.0
admin@Xorplus# commit
```

Usually, OSPF will try to form adjacencies with other routers on all interfaces that match the network prefix of an OSPF enabled interface. It is desirable to stop OSPF from forming adjacencies on interfaces facing the end users. To stop OSPF from forming adjacency on interface *vlan10*, run the command below.

```
admin@Xorplus# set protocols ospf instance-id 5 passive-interface vlan10
admin@Xorplus# commit
```

To redistribute BGP routes through an OSPF instance, run the command below.

```
admin@Xorplus# set protocols ospf instance-id 5 redistribute bgp
admin@Xorplus# commit
```

To configure OSPF SPF timers, run the commands shown below. This example configures the initial delay to 20ms, initial hold time to 100ms and the maximum hold time to 1000ms.

```
admin@Xorplus# set protocols ospf instance-id 5 timers throttle spf delay 20
admin@Xorplus# set protocols ospf instance-id 5 timers throttle spf initial-holdtime 100
admin@Xorplus# set protocols ospf instance-id 5 timers throttle spf maximum-holdtime 1000
admin@Xorplus# commit
```

And finally, to enable debugging information, run the below commands. These three commands enable debugging for Interface State Machine (ISM) events, the Link State Advertisement (LSA) flooding and the zebra module. For a full list of debugging options, please refer to the OSPFv2 command reference.

```
admin@Xorplus# set protocols ospf instance-id 5 traceoption ism events
admin@Xorplus# set protocols ospf instance-id 5 traceoption lsa flooding
admin@Xorplus# set protocols ospf instance-id 5 traceoption zebra
admin@Xorplus# commit
```

OSPF GR

- Overview
  - Device as a restarting device
  - Device as a Graceful Restart Helper
- Configuring OSPFv2 GR
  - Procedure
- Configuring OSPFv3 GR
  - Procedure
- Configuration Example
  - Networking Requirements
  - Procedure
    - Switch A
    - Switch B
    - Switch C
  - Verify the Configuration

NOTEs:

- PICOS supports Graceful Restart (GR) for both OSPFv2 and OSPFv3.
- Before configuring OSPF GR, you must enable OSPF's Opaque LSA capability by using the following command.

  For OSPFv2, using command **set protocols ospf [instance-id <***instance-id***>] [vrf**<*vrf-name*>**] capability opaque**.

  For OSPFv3, using command **set protocols ospf6 [instance-id <***instance-id***>] [vrf**<*vrf-name*>**] capability opaque**.
- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

Overview

OSPF GR (Graceful Restart) is a feature that allows a router to temporarily suspend OSPF routing operations without impacting the forwarding of data traffic. During a graceful restart, the router remains operational and continues forwarding packets using the routing information it had before OSPF protocol restarting process began.

In essence, OSPF GR allows a OSPF process to gracefully restart by preserving its OSPF neighbor relationships and forwarding state during the restart process.

Graceful restart is disabled by default. You can either globally enable graceful restart for all OSPF instances, or you can enable graceful restart for specific OSPF instance.

For a PICOS device, OSPF Graceful Restart involves the following operations:

Device as a restarting device

- In OSPF Graceful Restart (GR), a router that undergoes a restart process is referred to as the restarting router or restarting device. Here's a detailed description of its role and behavior during the GR process:
- **Restarting Process Initiation**: When a router undergoes a restart, it enters a restarting state. This can occur due to a planned restart (where the router voluntarily initiates the restart process) or an unplanned restart (such as a software upgrade or hardware failure).

a. **Neighbor State Maintenance**: During the restarting process, the router continues to maintain its OSPF neighbor adjacencies. It sends hello packets to its OSPF neighbors, indicating its restarting capability. These hello packets contain the Restart State (RS) bit, indicating that the router is in the process of restarting.
b. **Graceful Restart LSAs**: The restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain, informing its neighbors about its restarting process and the estimated time for the restart to complete. These LSAs are Type 9 LSAs and are flooded throughout the OSPF domain.
c. **State Retention**: Despite undergoing a restart, the restarting router retains its OSPF link-state database (LSDB) and continues forwarding traffic based on the pre-restart OSPF topology. This helps prevent service disruptions and maintains network stability during the restart process.
d. **Neighbor Acknowledgment**: OSPF neighbors of the restarting router acknowledge the reception of GR LSAs and adjust their behavior accordingly. They continue forwarding traffic through the restarting router, considering it as a transit router, until it completes the restart process and reestablishes full adjacency.
e. **Restart Completion**: Once the restarting router completes its restart process and is ready to resume normal operation, it sends OSPF hello packets without the RS bit set, indicating that it has completed the restart. It then reestablishes OSPF adjacencies with its neighbors and begins exchanging OSPF routing information.

- The restarting router in OSPF GR ensures seamless network operation during the restart process by maintaining adjacency with OSPF neighbors, advertising its restarting capability, and retaining its OSPF LSDB to continue forwarding traffic without disruption.

Device as a Graceful Restart Helper

- In OSPF Graceful Restart (GR), a router that assists a restarting router during its restart process is known as a Graceful Restart Helper. Here's a detailed description of its role and behavior:
- **Neighbor Detection**: When a router undergoing restart sends OSPF hello packets with the Restart State (RS) bit set, indicating its restarting status, neighboring routers detect this and voluntarily become Graceful Restart Helpers. They recognize the need to assist the restarting router to maintain network stability during the restart process.
  a. **LSDB Synchronization**: Graceful Restart Helpers maintain a synchronized copy of the restarting router's Link-State Database (LSDB). They ensure that they have the same set of OSPF LSAs as the restarting router before the restart process began.
  b. **Forwarding Continuity**: During the restart process, Graceful Restart Helpers continue to forward traffic through the restarting router as if it were still operational. They do this based on the pre-restart OSPF topology information stored in their LSDB. This ensures that network traffic flows smoothly without interruptions.
  c. **Designated Router Election**: In OSPF broadcast and non-broadcast networks, Graceful Restart Helpers participate in the election of Designated Routers (DR) and Backup Designated Routers (BDR). They help maintain the integrity of the OSPF network topology by ensuring that DR and BDR elections are conducted correctly even during the restarting router's downtime.
  d. **Monitoring Restart Progress**: Graceful Restart Helpers continuously monitor the progress of the restarting router's restart process. They keep track of the receipt of Graceful Restart (GR) Link-State Advertisements (LSAs) from the restarting router and maintain synchronization with its restart state.
  e. **Adjacency Retention**: Helpers maintain OSPF adjacencies with the restarting router throughout the restart process. They acknowledge the receipt of GR LSAs from the restarting router and adjust their behavior to accommodate its restarting status, ensuring seamless traffic forwarding.
  f. **Restart Completion Acknowledgment**: Once the restarting router completes its restart process and resumes normal operation, it sends OSPF hello packets without the RS bit set. Graceful Restart Helpers recognize this and acknowledge the completion of the restart. They then transition back to normal OSPF operation mode.

Graceful Restart Helpers play a critical role in assisting a restarting router to maintain network stability and continuity during the restart process. They synchronize LSDBs, ensure traffic forwarding, participate in DR/BDR elections, monitor restart progress, retain adjacencies, and acknowledge restart completion, contributing to the overall resilience and reliability of the OSPF network.

Configuring OSPFv2 GR

Procedure

Step 1 Enable the capability to generate Opaque LSAs in the OSPF process to support OSPF GR through Type9 LSA.

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] capability opaque**

Step 2 Enable OSPFv2 GR on the Restarting Router. By default, OSPFv2 GR is disabled.

set protocols ospf [**instance-id <***instance-id***>**] [**vrf**<*vrf-name*>] **graceful-restart enable** <**true** | **false**>

Step 3 (Optional) Specify the GR restart interval on the Restarting Router. This determines the duration for which the restarting router remains in the Graceful Restart state. The default grace period is 120 seconds.

set protocols ospf [**instance-id** <*instance-id*>] [**vrf**<*vrf-name*>] **grace-period <***grace-period***>**

Step 4 Configure GR Helper Mode on Neighboring Routers.

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

Step 5 (Optional) Configure Graceful Restart Helper parameters.

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper planned-only**

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper strict-lsa-checking enable <true | false>**

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper supported-grace-time <***supported-grace-time***>**

Step 6 Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

run graceful-restart prepare ospf

Step 7 Commit the configuration.

commit

Step 8 Verify the configuration.

After the configuration is complete, run **run show ospf** [**instance-id <***instance-id***>**][**vrf**<*vrf-name***>**] **graceful-restart helper [detail]** command to display the Graceful Restart Helper details including helper config changes.

By following these steps, you can configure OSPFv2 Graceful Restart to enhance network resilience and minimize service disruptions during router restarts.

Configuring OSPFv3 GR

Procedure

Step 1 Enable the capability to generate Opaque LSAs in the OSPF process to support OSPF GR through Type9 LSA.

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] capability opaque**

Step 2 Enable OSPFv3 GR on the Restarting Router. By default, OSPFv3 GR is disabled.

set protocols ospf6 [**instance-id <***instance-id***>**] [**vrf**<*vrf-name*>] **graceful-restart enable** <**true** | **false**>

Step 3 (Optional) Specify the GR restart interval on the Restarting Router. This determines the duration for which the restarting router remains in the Graceful Restart state. The default grace period is 120 seconds.

set protocols ospf6 [**instance-id** <*instance-id*>] [**vrf**<*vrf-name*>] **grace-period <***grace-period***>**

Step 4 Configure GR Helper Mode on Neighboring Routers.

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

Step 5 (Optional) Configure Graceful Restart Helper parameters.

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper planned-only**

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper lsa-checking-disable**

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper supported-grace-time <***supported-grace-time***>**

Step 6 Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPFv3 domain.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

run graceful-restart prepare ospf6

Step 7 Commit the configuration.

commit

Step 8 Verify the configuration.

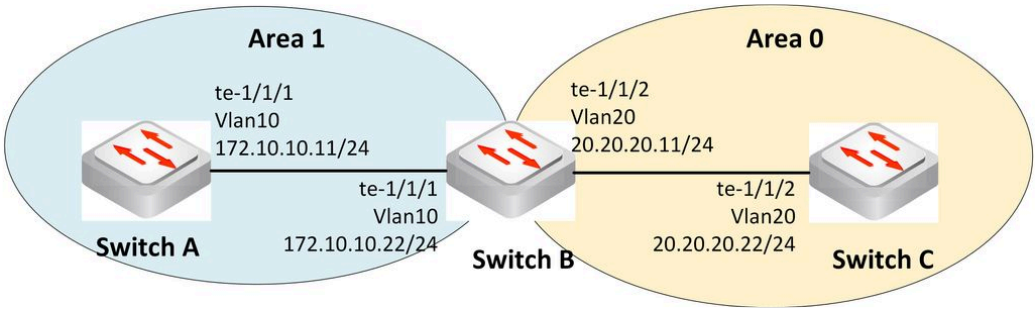
After the configuration is complete, run **run show ospf6** [**instance-id <***instance-id***>**][**vrf**<*vrf-name***>**] **graceful-restart helper [detail]** command to display the Graceful Restart Helper details including helper config changes.

By following these steps, you can configure OSPFv3 Graceful Restart to enhance network resilience and minimize service disruptions during router restarts.

Configuration Example

Networking Requirements

Figure 1. Network of Configuring OSPFv2 GR



As shown in **Figure 1**, the OSPF network is divided into two areas, Area 0 and Area 1, among the three devices running the OSPF protocol: Switch A, Switch B, and Switch C. It is now required that restarting the OSPF protocol on Switch A should not affect the normal data forwarding during the restart process.

The configuration approach is as follows:

1. Configure basic OSPF functions on each switch to achieve basic interoperability of OSPF networks.
2. Enable Opaque LSA function on Switch A and Switch B to enable OSPF to support OSPF GR through Type9 LSA.
3. Configure GR function on Switch A and Switch B to ensure normal data forwarding when OSPF protocol restarts.

Procedure

Switch A

Step 1 Configure the VLAN.

```
admin@SwitchA# set vlans vlan-id 10
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchA# set l3-interface vlan-interface vlan10 address 172.10.10.11 prefix-length 24
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf network 172.10.10.0/24 area 1
```

Step 3 Enable the capability to generate Opaque LSAs in the OSPF process to support OSPF GR through Type9 LSA.

```
admin@SwitchA# set protocols ospf capability opaque
```

Step 4 Enable OSPF GR on Switch A. By default, OSPF GR is disabled.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

```
admin@SwitchA# set protocols ospf graceful-restart enable true
```

Step 5 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step 1 Configure VLAN.

```
admin@SwitchB# set vlans vlan-id 10
admin@SwitchB# set vlans vlan-id 20
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchB# set l3-interface vlan-interface vlan10 address 172.10.10.22 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan20 address 20.20.20.11 prefix-length 24
admin@SwitchB# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node.

```
admin@SwitchB# set protocols ospf router-id 2.2.2.2
admin@SwitchB# set protocols ospf network 172.10.10.0/24 area 1
admin@SwitchB# set protocols ospf network 20.20.20.0/24 area 0
```

Step 3 Enable the capability to generate Opaque LSAs in the OSPF process to support OSPF GR through Type9 LSA.

```
admin@SwitchA# set protocols ospf capability opaque
```

Step 4 Configure GR Helper Mode on Switch B.

```
admin@SwitchB# set protocols ospf graceful-restart helper enable true
```

Step 5 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step 1 Configure VLAN.

```
admin@SwitchC# set vlans vlan-id 20
admin@SwitchC# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchC# set l3-interface vlan-interface vlan20 address 20.20.20.22 prefix-length 24
admin@SwitchC# set vlans vlan-id 20 l3-interface vlan20
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node.

```
admin@SwitchC# set protocols ospf router-id 3.3.3.3
admin@SwitchC# set protocols ospf network 20.20.20.0/24 area 0
```

Step 3 Commit the configuration.

```
admin@SwitchC# commit
```

Verify the Configuration

- After the configuration is complete, use command **run show ospf neighbor** to check the OSPF neighbor information. From the result, we can see that the neighbor state of Switch A and Switch B is **Full**.

```
admin@SwitchA# run show ospf neighbor
Neighbor ID     Pri State           Up Time         Dead Time Address         Interface
RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR         7m46s             35.806s 172.10.10.22    vlan10:172.10.10.11
0     0     0
admin@SwitchB# run show ospf neighbor
```

```
Neighbor ID     Pri State           Up Time         Dead Time Address         Interface
RXmtL RqstL DBsmL
1.1.1.1           1 Full/Backup     7m53s             36.400s 172.10.10.11    vlan10:172.10.10.22
0     0     0
3.3.3.3           1 Full/Backup     17m16s            33.592s 20.20.20.22     vlan20:20.20.20.11
0     0     0
```

- On Switch B, use command **run show ospf graceful-restart helper detail** to check the information of OSPF graceful restart helper. From the result, we can see that the negotiated OSPF GR information, including `Grace period`, `Remaining GraceTime`, etc.

```
admin@SwitchB# run show ospf graceful-restart helper detail
OSPF Router with ID (2.2.2.2)

 Graceful restart helper support enabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
 Last Helper exit Reason :Successful graceful restart
 Number of Active neighbours in graceful restart: 1
 Neighbour 1 :
   Address  : 172.10.10.11
   Routerid : 1.1.1.1
   Received Grace period : 120(in seconds).
   Actual Grace period : 120(in seconds)
   Remaining GraceTime:101(in seconds).
   Graceful Restart reason: Software restart.
```

- On Switch A, use the following Linux command to terminate the OSPF process. Then, the system will automatically restart the OSPF process.

```
root@SwitchA:/home/admin# pkill ospfd
```

- On Switch B, check the GR status. From the result, we can see that during the restart of `ospfd` on Switch A, the neighbor relationship between B and A remains in the **FULL** state, unaffected by the graceful restart of Switch A's OSPF process.

```
admin@SwitchB# run show ospf graceful-restart helper detail
OSPF Router with ID (2.2.2.2)

 Graceful restart helper support enabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
 Last Helper exit Reason :Successful graceful restart
 Number of Active neighbours in graceful restart: 1
 Neighbour 1 :
   Address  : 172.10.10.11
   Routerid : 1.1.1.1
   Received Grace period : 120(in seconds).
   Actual Grace period : 120(in seconds)
   Remaining GraceTime:86(in seconds).
   Graceful Restart reason: Software restart.

admin@SwitchB# run show ospf neighbor
Neighbor ID     Pri State           Up Time         Dead Time Address         Interface
RXmtL RqstL DBs
mL
1.1.1.1           1 Full/Backup     8m54s             36.507s 172.10.10.11    vlan10:172.10.10.22
0     0 0
```

```
22 3.3.3.3           1 Full/Backup     18m17s            32.987s 20.20.20.22     vlan20:20.20.20.11
   0     0 0
```

ECMP (Equal-Cost Multipath Routing) Configuration

NOTE:

- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.
- IPv6 static ECMP routing is not supported.

In L2/L3, ECMP is supported. The maximum ECMP outgoing port group is 4*128. If each ECMP route is configured to have up to 4 equal-cost paths, for example, the maximum ECMP outgoing port group support is 128. If each ECMP route is configured to have up to 16 equal-cost paths, the maximum ECMP outgoing port group support is 32. Several different ECMP routes can share the same outgoing port group. After configuring the ECMP equal-cost path maximum, reboot the switch to make it available.

Configuring the Equal-Cost Path Maximum

```
admin@XorPlus# set interface ecmp path_max 8
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
ECMP max path changes, please reset the box!
admin@XorPlus# run request system reboot
The system is going down NOW!
Sending SIGTERM to all processes
Sending SIGKILL to all processes
Requesting system reboot
Restarting system.
rstcr compatible register does not exist!
uses the mpc8541's gpio to do a reset.
U-Boot 1.3.0 (Sep 8 2010 - 17:20:00)
CPU: 8541, Version: 1.1, (0x80720011)
Core: E500, Version: 2.0, (0x80200020)
Clock Configuration:
CPU: 825 MHz, CCB: 330 MHz,
DDR: 165 MHz, LBC: 41 MHz
L1: D-cache 32 kB enabled
I-cache 32 kB enabled
I2C: ready
DRAM: Initializing
```

Configuring Static ECMP Routing

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set vlans vlan-id 4
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching native-vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 4
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set vlans vlan-id 4 l3-interface vlan-4
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.60.10 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.61.10 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-4 address 10.10.62.10 prefix-length 24
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols static route 10.10.51.0/24 next-hop 10.10.61.20
admin@XorPlus# set protocols static route 10.10.51.0/24 next-hop 10.10.62.20
admin@XorPlus# commit
Waiting for merging configuration.
```

```
Commit OK.
Save done.
```

Check the static ECMP route for 10.10.51.0/24 in the RIB with command **run show route ipv4**.

Configuring ECMP Hash Fields

In the default setting, all fields are hashed by IP-source, port-destination, port-source, and VLAN. Additional fields can be enabled, as shown below:

```
admin@XorPlus# set interface ecmp hash-mapping field ingress-interface disable false
admin@XorPlus# set interface ecmp hash-mapping field ip-destination disable false
admin@XorPlus# set interface ecmp hash-mapping field ip-protocol disable false
admin@XorPlus# set interface ecmp hash-mapping field ip-source disable false
admin@XorPlus# set interface ecmp hash-mapping field port-destination disable false
admin@XorPlus# set interface ecmp hash-mapping field port-source disable false
admin@XorPlus# set interface ecmp hash-mapping field vlan disable false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring ECMP Hash Mode

When you configure ECMP hash mode, follow these restrictions and guidelines:

- **round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, dlb-normal**, **dlb-optimal** and **dlb-assigned** for ECMP are only supported on **Trident3** and **Tomahawk3** platforms.
- **resilient-load-balancing** for ECMP is only supported on **Tomahawk2, Trident3-X7, Tomahawk3**, **Tomahawk4**, **Tomahawk5** and **Trident4** platforms.
- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

- Enable Randomized Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping randomized-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

- Enable round robin mode of ECMP load balancing.

```
admin@PICOS# set interface ecmp hash-mapping round-robin-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

- Enable normal mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

- Enable Symmetric Hash for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping symmetric true
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

- Enable Resilient Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping resilient-load-balancing
admin@PICOS# commit
admin@PICOS# exit
```

```
admin@PICOS> request system reboot
```

Symmetric Hash for ECMP Configuration Example

Symmetric Hash support for ECMP. Symmetric hash need the hashing field must be symmetric. For example, packet 1 and packet 2 are symmetric in table 1 and table 2 as below, and then packet 1 and packet2 will go out from the same physical port. Now Our symmetric Hash use IP layer and L4 field to hash when packets are transmitted on ECMP. Only matching symmetric condition, two packets can be transmitted on the same member port of ECMP.

IP Packet	Source IP Address	Destination IP Address
Packet1	10.1.1.1	20.1.1.1
Packet2	20.1.1.1	10.1.1.1

Table 1.

Layer 4 Packet	Source IP Address	Destination IP Address	Source Port Number	Destination Port Number
Packet1	10.1.1.1	20.1.1.1	100	200
Packet2	20.1.1.1	10.1.1.1	200	100

Table 2.

Symmetric Hash field as below:

1. ip-source
2. ip-destination
3. port-source
4. port-destination

By default, Enable hash field on ECMP:

1. ip-source
2. ip-destination
3. port-source
4. port-destination

> Symmetric hashing is supported on Helix4 **,** Trident2, Trident2+, Trident3 and Tomahawk platform switches.

ECMP Configuration

```
set interface ecmp hash-mapping symmetric true
```

ECMP Examples:

configure three ECMP route:

```
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 199
set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 299
set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 300
set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 301
set protocols static route 100.100.100.0/24 next-hop 182.168.1.100
set protocols static route 100.100.100.0/24 next-hop 183.168.1.100
set protocols static route 100.100.100.0/24 next-hop 184.168.1.100
set protocols static route 172.168.1.0/24 next-hop 182.168.1.100
set protocols static route 172.168.1.0/24 next-hop 183.168.1.100
set protocols static route 172.168.1.0/24 next-hop 184.168.1.100
set l3-interface vlan-interface vlan199 address 172.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan299 address 182.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan300 address 183.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan301 address 184.168.1.1 prefix-length 24
set l3-interface vlan-interface vlan399 address 100.100.100.1 prefix-length 24
set vlans vlan-id 199 l3-interface "vlan199"
set vlans vlan-id 299 l3-interface "vlan299"
set vlans vlan-id 300 l3-interface "vlan300"
set vlans vlan-id 301 l3-interface "vlan301"
set vlans vlan-id 399 l3-interface "vlan399"
```

Configure the symmetric hash true

```
set interface ecmp hash-mapping symmetric true
```

VRRP Configuration

- Principle of VRRP
- Configuration Notes of VRRP
- Configuring Standard VRRP
- Configuring Active-Active VRRP
- VRRP Configuration Example
  - Example for Configuring Standard VRRPv3 for IPv4
  - Example for Configuring Active-Active VRRPv3 for IPv4
  - Example for Configuring Active-Active VRRPv3 for IPv6

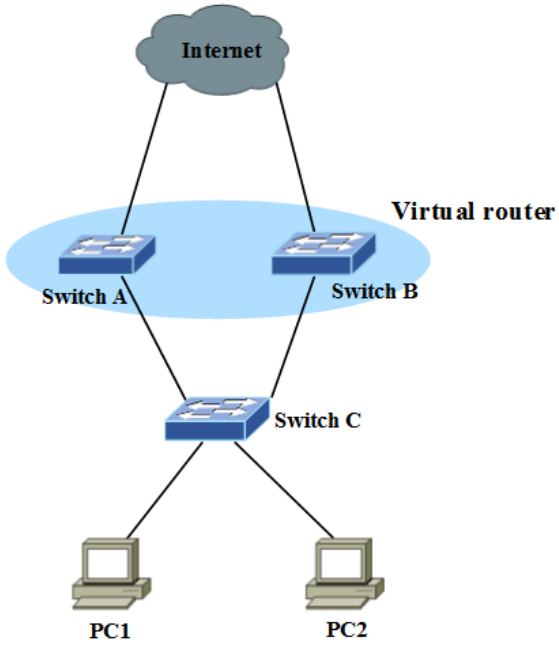
Principle of VRRP

- Introduction
- Active-Active VRRP Mode
  - VRRP Working Mechanism
  - VRRP Packet Format
  - VRRP Packet Types
  - VRRP States
  - Virtual MAC Address Allocation
  - Role Elect of Master and Backup
  - Virtual MAC Updating
  - ARP / IPv6 Neighbor synchronization
  - Accept Mode

Introduction

Virtual Router Redundancy Protocol (VRRP) is a redundancy and backup function of network devices. VRRP group combines several routing devices into one virtual routing device and uses the IP address of the virtual routing device as the default gateway to establish communication with external networks. When a gateway device in a VRRP group fails, the VRRP mechanism can elect a new gateway device as Master to transmit the data traffic to ensure reliable network communication.

Figure 1. VRRP Networking Diagram



As shown in Figure 1, Switch A and Switch B form a virtual router. This virtual router has its own IP (could be IPv4 or IPv6) address. The hosts in the LAN use the virtual router IP as their default gateway IP. The switch with the highest priority between Switch A and Switch B functions as the master and the gateway device. The other switch functions as the backup router. For IPv4, the VRRP packets will use multicast MAC 01:00:5E:00:00:12 as destination MAC. For IPv6, the VRRP packets will use multicast MAC 33:33:00:00:00:12 as destination MAC. Switch C should support layer 2 switching function.

Besides the Standard VRRP protocol mode, PICOS also supports Active-Active VRRP mode. In the Standard VRRP protocol mode, only the Virtual Master Router can forward packets whereas the Virtual Backup Routers cannot forward packets. By adding a new working mechanism based on the VRRP standard protocol mode, Active-Active VRRP mode provides load balancing between the master and backup switches in the VRRP group, both of which are active, thus avoid the situation where the backup switches are always idle in the Standard VRRP protocol mode. This greatly improves usage efficiency of network resources.

In the version before PICOS 2.11.10, PICA8 switch supports only VRRPv2. From PICOS 2.11.10, PICA8 switch supports both VRRPv2 and VRRPv3. The differences between VRRPv2 and VRRPv3 are as follows:

- Apply to different networks. VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses.
- Packet format is different between VRRPv2 and VRRPv3, for details please refer to VRRP Packet Format.
- VRRPv3 supports accept mode while VRRPv2 does NOT support this mode. Accept mode controls whether a virtual router in master state will accept packets addressed to the virtual IPvX address of the VRRP group if it is not the IP address owner. However, in VRRPv2, the master switch always accepts packets addressed to the virtual IPvX address. For details about accept mode, please refer to Accept Mode.

NOTE:

- VRRPv2 and VRRPv3 interoperation is not supported, VRRP version configured on all devices in a VRRPv3 group must be the same.
- Standard VRRP mode supports one Master and several Backup switches in a VRRP group, while Active-Active VRRP mode supports only one Master and one Backup switch in a VRRP group.
- The same VRID must be configured on all devices for the same VRRP group.

- The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is same as the virtual IP address is called an "IP address owner". When the router is an IP address owner, its priority is always 255.
- Only one IP address owner can be configured in the same VRRP group.

The VRRP principle included in this document describes only the working mechanism of Active-Active VRRP mode for IPvX (In this document, the term "IPvX" (where X is 4 or 6) is introduced to mean either "IPv4" or "IPv6"). For details about standard VRRPv2 protocol mode, please refer to the RFC3768. For details about Standard VRRPv3 protocol mode, please refer to RFC5798.

Active-Active VRRP Mode

The basic principle in Active-Active VRRP is that one virtual IPvX address corresponds to two virtual MAC addresses, and each switch in the VRRP group corresponds to one virtual MAC address to support load balancing between the master and backup switches. This helps in avoiding the backup switch from being in idle state as is the case in Standard VRRP mode.

VRRP Working Mechanism

Active-Active VRRP mode working process is as follows:

1. Devices in a VRRP group elect the Master and Backup based on their priorities and VLAN interface/routed interface IPvX addresses by exchanging VRRP advertisement packets.

2. The master and backup devices periodically send VRRP Advertisement packets to each other to advertise its configuration (such as priority) and running status. This can also notify the downstream devices to refresh the MAC entries.

3. All the ARP requests / Neighbor Solicitation (NS) packets from the downstream devices or hosts are responded to by the master. ARP reply / Neighbor Advertisement (NA) packets carry one of the virtual MAC addresses of the VRRP group. For details about virtual MAC address allocation, please see Virtual MAC Address Allocation.

4. To notify the downstream devices of the virtual MAC, the master and backup devices periodically send virtual MAC update messages. For details, please refer to Virtual MAC Updating.

5. For IPv6, master sends Router Advertisements for the link-local addresses of virtual router IP address on the local area network to announce its availability for routing.

6. The VRRP device uses its real MAC address as source MAC for traffic forwarding.

VRRP Packet Format

VRRP packets are sent encapsulated in IPvX packets. For IPv4, in Layer 3 IP header of VRRP packets, source IP is the real IP (same segment with Virtual IP) of the VLAN interface/routed interface, destination IP is IPv4 multicast address 224.0.0.18 that is assigned to VRRP. In Ethernet header, source MAC is virtual MAC, and destination MAC is multicast MAC 01:00:5E:00:00:12. For IPv6, destination IP is IPv6 multicast address FF02::12 and destination MAC is multicast MAC 33:33:00:00:00:12.

VRRPv2 and VRRPv3 packet formats are shown below.

Figure 2. VRRPv2 Packet

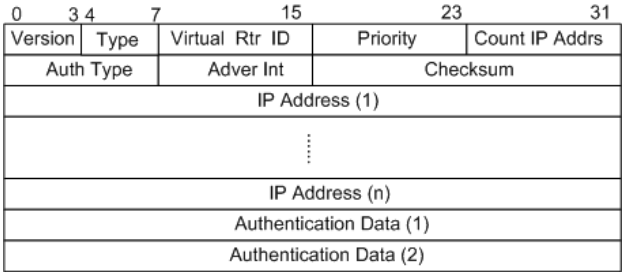


Figure 3. VRRPv3 Packet

VRRP Field	Descriptions
Version	The version field specifies the VRRP protocol mode. • VRRP_VERSION = 2, Standard VRRPv2 mode. • VRRP_VERSION = 3, Standard VRRPv3 mode. • VRRP_LOAD_BALANCE_VERSION = 4, Active-Active VRRPv2 mode. • VRRP_LOAD_BALANCE_VERSION = 5, Active-Active VRRPv3 mode.

Type	The type field specifies the type of VRRP packet. • VRRP_TYPE_ADVERTISEMENT = 1, advertisement packet sent by the master. • VRRP_BACKUP_ADVERTISEMENT = 2, advertisement packet sent by the backup device. • VRRP_UPDATE_ADVERTISEMENT = 3, MAC address update packet, sent periodically both by the master and backup devices. • VRRP_SYNC_ARP_ADVERTISEMENT / VRRP_SYNC_ NEIGHBOR_ADVERTISEMENT = 4, ARP synchronization /IPv6 Neighbor synchronization packet.
Virtual Rtr ID	Virtual router ID, range from 1 to 254.
Priority	Device priority in the VRRP group, range from 1 to 254. The default value is 100.
Count IP Addrs / Count IPvX Addr	The number of virtual IPvX addresses in the VRRP group.
Auth Type	Used only for VRRPv2 packets. The authentication type field identifies the authentication method being utilized. There are three types: • 0: Non Authentication. • 1: Simple Text Password. • 2: IP Authentication Header, which indicates the MD5 authentication mode. By default, there's no authentication.
rsvd	Reserved field for VRRPv3 packets.
Adver Int / Max Adver Int	VRRP advertisement interval, in second for IPv4 network and centisecond for IPv6 network. The default value is 4 seconds for both IPv4 and IPv6.
Checksum	The checksum field is used to detect data corruption in the VRRP packet.
IP Address / IPvX Addresses	IPvX address list that is associated with the virtual router. The number of addresses included is specified in the "Count IPvX Addr" field.
Authentication Data	Authentication key.

VRRP Packet Types

There are four types of VRRP packets in Active-Active VRRP mode: master advertisement, backup advertisement, virtual MAC update packet, and ARP synchronization / IPv6 neighbor synchronization packet.

1) Master advertisement where type = 1

The master device periodically sends VRRP advertisement packets to the backup device to advertise its configuration information (such as priority) and working status. The backup device determines whether the master is working properly by receiving VRRP advertisement packets.

When the master device fails to send advertisement packets due to some network fault, the backup device can not immediately get the working status of the master. It will wait until the Master_Down_Interval timer expires before it considers that the master device has failed, then switches its own state to Master. The value of the Master_Down_Interval timer is 3 × Advertisement_Interval + Skew_time, Skew_Time = (256 - Priority)/256, in seconds.

2) Backup advertisement message where type = 2

Backup device periodically sends VRRP advertisements to advertise its configuration information (such as priority) and working status in the VRRP group. The master device determines whether the backup device is working properly by receiving Backup advertisement packets. The interval for sending advertisement messages is the same as that of the Master advertisement message.

3) Virtual MAC update message where type = 3

To notify the downstream devices of the virtual MAC, the master and backup devices periodically send virtual MAC update messages. The virtual MAC address in Active-Active VRRP mode is used in the Ethernet header of virtual MAC update packet as the source MAC address. The connected network devices of the VRRP group refresh the MAC entries in time to perform packet forwarding. The default interval is 120s.

4) ARP synchronization message or IPv6 neighbor synchronization where type = 4

The VRRP device learns ARP entries / IPv6 Neighbor entries from the receiving traffic.

In order to ensure that both devices in the VRRP group can forward downstream data rapidly, ARP **/** IPv6 Neighbor synchronization packets are sent between the Master and Backup device when the ARP **/** IPv6 Neighbor table on the VRRP group device is updated.

For IPv4, the IPv4 addresses in the ARP table that are in the same network segment with virtual IPv4 address are synchronized to the peer VRRP device.

For IPv6, two types of IPv6 address in the Neighbor table are synchronized to the peer VRRP device,

- The global IPv6 addresses in the IPv6 Neighbor table that are in the same network segment with virtual IPv6 address.
- The link-local addresses that are in the same VLAN with the VRRP group.

Upon receiving the ARP synchronization **/** IPv6 Neighbor synchronization packet, the peer device initiates ARP **/** IPv6 Neighbor learning process. The ARP **/** IPv6 Neighbor entries on both VRRP devices will eventually reach a consistent state and both devices in the VRRP group can forward downstream data rapidly.

VRRP States

VRRP protocol defines three state machines: Initialize, Master and Backup.

Initialize

- VRRP is unavailable. The device in Initialize state cannot process VRRP advertisement packets.
- When the VRRP process starts it goes into initialize state. When the device is in master or backup states and it detects a fault, it enters the Initialize state.

- After receiving an interface Up message, the VRRP-enabled device first switches to the Backup state and then switches to the Master state after the Master_Down_Interval timer expires.

Master

The VRRP device in Master state performs the following operations:

- Sends VRRP advertisement packets periodically.
- Receives VRRP advertisement packets from the backup and determines whether the backup is working properly.
- Uses the virtual MAC address to respond to ARP request destined for the virtual IPv4 address.
- Uses the virtual MAC address to respond to ND Neighbor Solicitation messages destined for the virtual IPv6 address.
- Forwards IPvX packets destined for the virtual MAC address.
- Becomes the backup if the device receives a VRRP advertisement packet with a higher priority than its VRRP priority.
- Becomes the backup if the device receives a VRRP advertisement packet with the same priority as its VRRP priority and the local VLAN interface/routed interface address is smaller than the connected interface address on the peer VRRP device.
- For VRRPv3, accepts packets addressed to the IPvX address(es) associated with the virtual router if it is the IPvX address owner or if Accept Mode is True. For details about Accept Mode, please see Accept Mode.
- Sends Router Advertisement for the link-local addresses in virtual IP address list, as the source IP address of the RA packet, on the local area network to announce its virtual IP address as available for routing. In the prefix information field of the RA packet, it carries the global addresses in virtual IP address list for applying IPv6 stateless address auto-configuration protocol (refer to RFC2462 IPv6 Stateless Address Autoconfiguration).

Backup

The VRRP device in Backup state performs the following operations:

- Sends VRRP advertisement packets periodically.
- Receives VRRP advertisement packets from the master and determines whether the master is working properly.
- Does NOT respond to ARP request / ND Neighbor Solicitation messages destined for the virtual IPv4 / IPv6 address.
- Forwards IPvX packets destined for the virtual MAC address in Active-Active mode for load balancing.
- When it receives a packet of lower priority, it immediately switches to the Master state by default. If non-preemptive is configured, the device remains in the backup state.
- Master_Down_Interval timer: If the backup receives no advertisement packet after the timer expires, the backup takes the role of the master. The calculation formula is as follows:

  Master_Down_Interval = 3*Advertisement_Interval + Skew_time (offset time)

  Skew_Time = (256 - Priority) / 256
- For VRRPv3, does NOT accept packets addressed to the IPvX address(es) associated with the virtual router.
- Does NOT send Router Advertisement messages for the virtual router.

Virtual MAC Address Allocation

In Active-Active VRRP mode, the master switch no longer sends gratuitous ARP request or unsolicited ND Neighbor Advertisement packets as Standard VRRP protocol mode does. Instead, the master switch receives the ARP request / ND Neighbor Solicitation message sent by the connected hosts or devices and responds with ARP reply / ND Neighbor Solicitation message using the virtual MAC address instead of the real MAC address of the interface.

The virtual MAC address is allocated according to the hash value calculated from the source MAC address in the ARP request packet / ND Neighbor Solicitation message. This results in half of the hosts end up learning the virtual MAC address of Master and the other half of the hosts learn the virtual MAC address of the Backup. In this way, traffic from the hosts is shared between two VRRP devices to achieve load balancing.

The virtual router generates the virtual MAC address based on the virtual router ID, the format is 00: 00: 5E: 00: 0X: VRID. For IPv4, X is 1 in master device and 2 in backup device; For IPv6, X is 2 in master device and 1 in backup device.

For example, assuming that VRID 5 enables Active-Active VRRP mode for IPv4 and VRID 6 enables Active-Active VRRP mode for IPv6, then the virtual MAC addresses of VRID 5 will be 00-00-5E-00-01-05 and 00-00-5E-00-02-05, and that of VRID 6 will be 00-00-5E-00-02-06 and 00-00-5E-00-01-06.

Role Elect of Master and Backup

VRRP determines the device role in the VRRP group based on device priority and VLAN interface/routed interface by exchanging VRRP advertisement packets. The device with a higher priority is more likely to become the master. If two devices have the same priority, the device with a larger VLAN interface/routed interface IP address becomes the master.

The VRRP-enabled device in a VRRP group initially works in Initialize state. After receiving an interface Up message, if the priority of the device is 255, it will become the master directly; if the priority of the device is less than 255, the VRRP-enabled device first switches to the Backup state and then switches to the Master state when the Master_Down_Interval timer expires.

The device that first switches to the Master state obtains the priorities of other devices in the group by exchanging VRRP advertisement packet and then elect the master router.

- If the master priority in VRRP advertisement packets is higher than or equal to the priority of the device, the backup remains in Backup state.
- If the backup device has a higher priority than the master, the working mode of the backup (preemptive or non-preemptive) determines whether the master is re-elected.
  - Preemptive mode: If the priority of the backup router is higher than the priority of the current master router, the backup router automatically becomes the master router.
  - Non-preemptive mode: As long as the master router is working properly, the backup router with a higher priority cannot become the master router.
- The IP address owner's running priority is always 255; the IP address owner always works in preemptive mode, regardless of whether the preemption function is enabled. If the VRRP device is the IP address owner, it will switch to the master state immediately after receiving the interface Up message.

Virtual MAC Updating

To notify the downstream devices of the virtual MAC, the master and backup devices periodically send virtual MAC update messages. The virtual MAC address in Active-Active VRRP mode is used in the Ethernet header of virtual MAC update packet as the source MAC address. The connected network devices of the VRRP group refresh the MAC entries in time to perform packet forwarding. The default interval is 120s.

ARP / IPv6 Neighbor synchronization

The VRRP devices learn ARP entries / IPv6 Neighbor entries when receiving downstream traffic.

In order to ensure that both devices in the VRRP group can forward downstream data rapidly, ARP **/** IPv6 Neighbor synchronization packets are sent between the Master and Backup device when the ARP **/** IPv6 Neighbor table on the VRRP group device is updated.

For IPv4, the IPv4 addresses in the ARP table that are in the same network segment with virtual IPv4 address are synchronized to the peer VRRP device.

For IPv6, two IP addresses in the Neighbor table are synchronized to the peer VRRP device,

- The global IPv6 addresses in the IPv6 Neighbor table that are in the same network segment with virtual IPv6 address.
- The link-local addresses that are in the same VLAN with the VRRP group.

Upon receiving the ARP synchronization **/** IPv6 Neighbor synchronization packet, the peer device initiates ARP **/** IPv6 Neighbor learning process. The ARP **/** IPv6 Neighbor entries on both VRRP devices will eventually reach a consistent state and both devices in the VRRP group can forward downstream data rapidly.

Accept Mode

VRRPv3 supports Accept Mode which controls whether a virtual router in Master state will accept packets addressed to the virtual IPvX address of a VRRP group if it is not the IP address owner (the IP address owner is the router that has the interface whose actual IP address is used as the virtual router's IP address).

By default, the Accept Mode is disabled, if the master is not the IP address owner, it only accepts the ARP requests/ARP replies or NS/NA messages addressed to the virtual IP, any other messages whose destination IP is the virtual IP are not accepted. But when accept mode is enabled, it can accept all packets whose destination IP is a virtual IP.

Deployments that rely on, for example, pinging the address owner's IPvX address may choose to configure Accept Mode to True.

NOTE:

- Accept Mode is only supported in VRRPv3 while VRRPv2 does NOT support. In VRRPv2, the master switch always accepts packets addressed to the virtual IPvX address.
- When Accept Mode is disabled, PICOS can still accept and process IPv6 Neighbor Solicitations / Neighbor Advertisements packets and ARP Request / ARP Reply packets.
- If the master is the IP address owner, it accepts all the packets addressed to the IPvX address(es) associated with the virtual router even though Accept Mode is disabled.

Configuration Notes of VRRP

When configuring VRRP on a device, pay attention to the following points:

- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.
- VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses.
- As VRRPv2 and VRRPv3 interoperation is not supported, VRRP version must be the same on both devices in a VRRP group. If the VRRP versions on the switches in the same VRRP group are different, it may cause VRRP communication to fail.
- When upgrading, we recommend that PICOS versions of the VRRP group devices be upgraded to PICOS 2.11.10 or later versions at the same time, as PICOS supports VRRPv3 from PICOS 2.11.10.
- VRRP supports VRF function by binding the Layer 3 interface to a specified VRF.
- The following configurations must be identical on both devices in the same VRRP group,
  - VRRP version.
  - Interval of sending VRRP advertisement packets.
  - Virtual IPvX lists.
  - Active-Active VRRP mode. You should either enable or disable Active-Active VRRP mode on both VRRP devices.
  - Authentication mode and authentication key.
- Active-Active VRRP mode supports only one Master and one Backup switch in a VRRP group. Standard VRRP mode supports one Master and several Backup switches in a VRRP group.
- One chassis switch supports a maximum of 128 VRRP groups. Please set the number of VRRP group based on device performance.
- One VRRP group supports a maximum of 254 virtual IPv4 addresses, and 64 virtual IPv6 addresses.
- Follow the rules below when configuring the virtual IPv4 / IPv6 address:
  - For IPv4, the virtual IPv4 of the VRRP group and the IPv4 address of the interface should be configured in the same network segment to ensure that the VRRP group can work normally.
  - The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is the same as the virtual IP address is called an "IP address owner".
  - The virtual IPv4 address of the VRRP group cannot be all zeros, broadcast address (255.255.255.255), network address or network broadcast address of the segment where the virtual IP address resides, loopback address, non-A / B / C address or any other illegal IP Address (e.g., 0.0.0.1).
  - For IPv6, the global virtual IPv6 address of the VRRPv3 group and the global IPv6 address of the interface should be configured in the same network segment to ensure that the VRRPv3 group can work normally.
  - In one VRRP group, IPv4 and IPv6 networks cannot be mixed. That is, the configured virtual IP addresses in the same VRRP group could either be IPv4 addresses or IPv6 addresses.
  - For IPv6, configure at least one link-local IPv6 address in a VRRPv3 group which will be used as the gateway address for the hosts, the format is FE80::/10.
  - Virtual IP address list on both devices of VRRP group must be the same.
  - Configure one or more global virtual IPv6 addresses, for the purpose of configuring global addresses via stateless address autoconfiguration of the downstream host (refer to RFC2462 IPv6 Stateless Address Autoconfiguration).
- The gateway address of the downstream host should be configured as the virtual IPvX address of the VRRP virtual router device. For IPv6, the gateway address should be the virtual link-local address.
- IPv4 address of Layer 3 interfaces in a VRRP group should be configured within the same network segment.
- Two devices in a VRRP group must be configured with the same VRID.
- It is recommended that VRRP groups on different L3 interfaces of a device should be configured with a different VRIDs.
- VRRPv3 protocol and the function of sending Router Advertisement message cannot be configured at the same time, as VRRPv3 master device could send Router Advertisements for the link-local addresses in virtual IP address list. Before you enable VRRPv3, disable sending RA message by using the command **set l3-interface vlan-interface** <*interface-name*> **ipv6-nd suppress-ra true** or **set l3-interface routed-interface** <*interface-name*> **ipv6-nd suppress-ra true**.
- When Accept Mode is disabled, PICOS can still accept and process IPv6 Neighbor Solicitations / Neighbor Advertisements packets and ARP Request / ARP Reply packets.

Configuring Standard VRRP

Procedure

Step1 Configure Layer 3 interface. VRRP can be enabled on a VLAN interface or a routed interface.

- Configure a VLAN interface.

  a) Configure VLAN ID.

  set vlans vlan-id <*vlan-id*>

  b) Configure the interface to VLAN.

  set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

  c) Configure the IP address of the VLAN.

  set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

  d) Associate a Layer 3 interface with a VLAN.

  set vlans vlan-id <vlan-id> **l3-interface** <*interface-name*>

- Configure a routed interface.

  a) Enable routed interface.

  set interface gigabit-ethernet <*interface-name*> **routed-interface enable** <**true | false**>

  set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

  b) Configure reserved-vlan for the routed interface.

  set vlans reserved-vlan <*reserved-vlan*>

  c) (Optional) Create the sub-interface and add it into a VLAN.

  set interface aggregate-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

  d) Configure the IP address of the routed interface.

  set l3-interface routed-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix-number*>

Step2 Create a VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*>

NOTE:

- Two devices in a VRRP group must be configured with the same VRID.
- One chassis switch supports a maximum of 128 VRRP groups. Please set the number of VRRP group based on device performance.
- It is recommended that VRRP groups on different L3 interfaces of a device should be configured with different VRIDs.

Step3 Enable the VRRP function.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **disable** <**true | false**>

By default, the VRRP function is enabled. Currently, VRRP can be configured on the VLAN interfaces or routed interfaces.

Step4 Configure the VRRP version number.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **version** <**2** | **3**>

By default, the system uses VRRPv2.

Step5 Configure a virtual IP address for the VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ip** <*ipv4-address*>

NOTE:

- One VRRP group supports a maximum of 254 virtual IPv4 addresses, and 64 virtual IPv6 addresses.
- For IPv4, the virtual IPv4 address of the VRRP group and the IPv4 address of the interface should be configured in the same network segment to ensure that the VRRP group can work normally.
- The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is the same as the virtual IP address is called an "IP address owner".
- The virtual IPv4 address of the VRRP group cannot be all zeros, broadcast address (255.255.255.255), network address or network broadcast address of the segment where the virtual IP address resides, loopback address, non-A / B / C address or any other illegal IP Address (e.g., 0.0.0.1).
- For IPv6, the global virtual IPv6 address of the VRRPv3 group and the global IPv6 address of the interface should be configured in the same network segment to ensure that the VRRPv3 group can work normally.
- In one VRRP group, IPv4 and IPv6 networks cannot be mixed. That is, the configured virtual IP addresses in the same VRRP group could either be IPv4 addresses or IPv6 addresses.
- For IPv6, configure at least one link-local IPv6 address in a VRRPv3 group which will be used as the gateway address for the hosts, the format is FE80::/10.
- Virtual IP address list on both devices of VRRP group must be the same.

- Configure one or more global virtual IPv6 addresses, for the purpose of configuring global addresses via stateless address autoconfiguration of the downstream host refer to RFC2462 IPv6 Stateless Address Autoconfiguration.

Step6 (Optional) Configure the interval of sending VRRP advertisement packets.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **interval** <*interval-value*>

NOTE:

- By default, the value is 4 seconds.
- The configurations of the interval of sending VRRP advertisement packets on both devices of VRRP group must be the same.

Step7 (Optional) Configure VRRP preemptive mode.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **preempt enable** <**true | false**>

By default, preemptive mode is enabled.

Step8 (Optional) Configure the priority of the device in a VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **priority** <*priority-value*>

By default, the priority of the device in a VRRP group is 100.

Step9 (Optional) Configure an authentication mode and authentication key for a VRRP group. Note that VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication type** <**none** | **md5** | **simple**>

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication simple-key** <*simple-key*>

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication md5-key** <*md5-key*>

Step10 (Optional) Enable accept mode.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **accept disable** <**true** | **false**>

NOTE:

- Accept mode is only supported in VRRPv3.
- By default, accept mode is disabled.

Step10 (Optional) Configure the paremeters for sending router advertisement messages.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd** *xx*

Configuring Active-Active VRRP

Procedure

Step1 Configure Layer 3 interface. VRRP can be enabled on a VLAN interface or a routed interface.

- Configure a VLAN interface.

  a) Configure VLAN ID.

  set vlans vlan-id <*vlan-id*>

  b) Configure the interface to VLAN.

  set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

  c) Configure the IP address of the VLAN.

  set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

  d) Associate a Layer 3 interface with a VLAN.

  set vlans vlan-id <vlan-id> **l3-interface** <*interface-name*>

- Configure a routed interface.

  a) Enable routed interface.

  set interface gigabit-ethernet <*interface-name*> **routed-interface enable** <**true | false**>

  set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

  b) Configure reserved-vlan for the routed interface.

  set vlans reserved-vlan <*reserved-vlan*>

  c) (Optional) Create the sub-interface and add it into a VLAN.

  set interface aggregate-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

  d) Configure the IP address of the routed interface.

  set l3-interface routed-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix-number*>

Step2 Create a VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*>

NOTE:

- Two devices in a VRRP group must be configured with the same VRID.
- One chassis switch supports a maximum of 128 VRRP groups. Please set the number of VRRP group based on device performance.
- It is recommended that VRRP groups on different L3 interfaces of a device should be configured with different VRIDs.

Step3 Configure the VRRP version number.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **version** <**2** | **3**>

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **disable** <**true | false**>

By default, the VRRP function is enabled. Currently, VRRP can be configured on the VLAN interfaces or routed interfaces.

Step5 Enable the Active-Active VRRP function.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance disable** <**true | false**>

NOTE:

- By default, the Active-Active VRRP function is disabled.
- The setting of enabling Active-Active VRRP must be the same on both devices of VRRP group.

Step6 Configure a virtual IP address for the VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ip** <*ipv4-address*>

NOTE:

- One VRRP group supports a maximum of 254 virtual IPv4 addresses, and 64 virtual IPv6 addresses.
- For IPv4, the virtual IPv4 address of the VRRP group and the IPv4 address of the interface should be configured in the same network segment to ensure that the VRRP group can work normally.
- The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is the same as the virtual IP address is called an "IP address owner".
- The virtual IPv4 address of the VRRP group cannot be all zeros, broadcast address (255.255.255.255), network address or network broadcast address of the segment where the virtual IP address resides, loopback address, non-A / B / C address or any other illegal IP Address (e.g., 0.0.0.1).

- For IPv6, the global virtual IPv6 address of the VRRPv3 group and the global IPv6 address of the interface should be configured in the same network segment to ensure that the VRRPv3 group can work normally.
- In one VRRP group, IPv4 and IPv6 networks cannot be mixed. That is, the configured virtual IP addresses in the same VRRP group could either be IPv4 addresses or IPv6 addresses.
- For IPv6, configure at least one link-local IPv6 address in a VRRPv3 group which will be used as the gateway address for the hosts, the format is FE80::/10.
- Virtual IP address list on both devices of VRRP group must be the same.
- Configure one or more global virtual IPv6 addresses, for the purpose of configuring global addresses via stateless address autoconfiguration of the downstream host refer to RFC2462 IPv6 Stateless Address Autoconfiguration.

Step7 (Optional) Configure the interval of sending VRRP advertisement packets.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **interval** <*interval-value*>

NOTE:

- By default, the value is 4 seconds.
- The configurations of the interval of sending VRRP advertisement packets on both devices of VRRP group must be the same.

Step8 (Optional) Configure VRRP preemptive mode.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **preempt enable** <**true | false**>

By default, preemptive mode is enabled.

Step9 (Optional) Configure the interval of updating the virtual MAC.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance virtual-MAC time-interval** <*interval-value*>

Step10 (Optional) Configure the priority of the device in a VRRP group.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **priority** <*priority-value*>

By default, the priority of the device in a VRRP group is 100.

Step11 (Optional) Configure an authentication mode and authentication key for a VRRP group. Note that VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication type** <**none** | **md5** | **simple**>

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication simple-key** <*simple-key*>

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication md5-key** <*md5-key*>

Step12 (Optional) Enable accept mode.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **accept disable** <**true** | **false**>

NOTE:

- Accept mode is only supported in VRRPv3.
- By default, accept mode is disabled.

Step13 (Optional) Configure the paremeters for sending router advertisement messages.

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd** *xx*

VRRP Configuration Example

- Example for Configuring Standard VRRPv3 for IPv4
- Example for Configuring Active-Active VRRPv3 for IPv4
- Example for Configuring Active-Active VRRPv3 for IPv6

Example for Configuring Standard VRRPv3 for IPv4

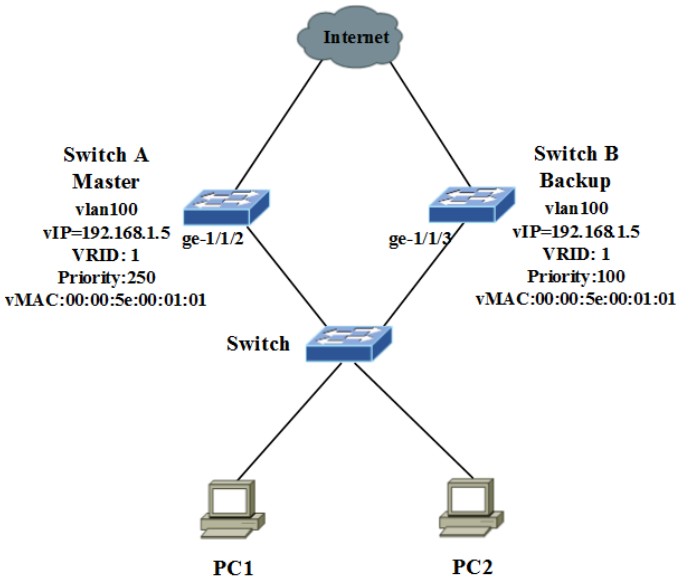
- Networking Requirements
- Procedure
  - Switch A
  - Switch B
- Verify the Configuration

Networking Requirements

In figure 1, Switch connects to the internet through gateway switches Switch A and Switch B. To ensure nonstop service availability, a VRRP group in standard mode needs to be configured on SwitchA and SwitchB.

- Configure the VRRP router ID as 1, Switch A is the Master and Switch B is the Backup switch of VRRP group.
- The virtual IP of VRRP router is 192.168.1.5, virtual MAC is 00:00:5e:00:01:01.
- The gateway address of the downstream host PC1 and PC2 needs to be configured as the IP address of the VRRP virtual router device.

Figure 1. Networking of Standard VRRP



Procedure

Switch A

Step1 Configure VLAN.

admin@SwitchA# set vlans vlan-id 100

admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100

admin@SwitchA# set l3-interface vlan-interface vlan100 address 192.168.1.1 prefix-length 24

admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchA#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Configure a virtual IP address for the VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5

Step6 Configure the priority of a device in a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 priority 250

Step7 Commit the configuration.

admin@SwitchA# commit

Switch B

Step1 Configure VLAN.

admin@SwitchB# set vlans vlan-id 100

admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 100

admin@SwitchB# set l3-interface vlan-interface vlan100 address 192.168.1.2 prefix-length 24

admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchB#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Configure a virtual IP address for the VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5

Step6 Configure the priority of the device in a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 priority 100

Step7 Commit the configuration.

admin@SwitchB# commit

Verify the Configuration

- After the configuration is complete, run **run show vrrp** command to view the configuration information of VRRP group. The result of show command on the master is as follows.

```
admin@SwitchA# run show vrrp
Interface:                    vlan100
VRID:                         1
Version:                      3
Load-balance:                 disable
State:                        Master
Master IP:                    192.168.1.1
Virtual MAC:                  00:00:5e:00:01:01
Preempt:                      enable
Adver Interval:               4
Priority:                     250
Virtual IP:                   192.168.1.5
Auth-type:                    none
Auth-key:
```

- When showing MAC address table on the downstream switch to check the MAC address of the device, you can see the virtual MAC entries corresponding to the virtual IP address of the VRRP group.
- On PC1 and PC2, ping the virtual IP address 192.168.1.5 to check the connectivity with the devices in VRRP group.

Example for Configuring Active-Active VRRPv3 for IPv4

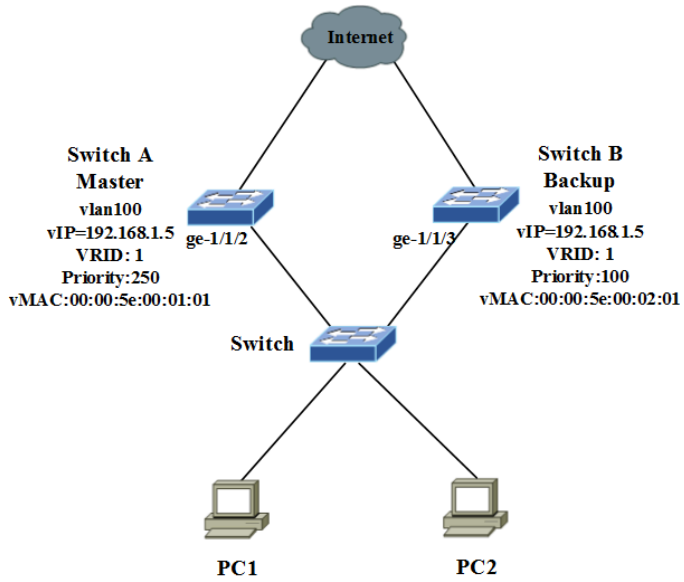
- Networking Requirements
- Procedure
  - Switch A
  - Switch B
- Verify the Configuration

Networking Requirements

In figure 1, Switch connects to the internet through gateway switches Switch A and Switch B. To ensure nonstop service availability, a VRRP group in Active-Active mode needs to be configured on SwitchA and SwitchB.

- Configure the VRRP router ID as 1, Switch A is the master and Switch B is the backup switch of VRRP group.
- The virtual IP of VRRP virtual router is 192.168.1.5, virtual MAC on master switch is 00:00:5e:00:01:01 and 00:00:5e:00:02:01 on the backup switch.
- The gateway address of the downstream host PC1 and PC2 needs to be configured as the IP address of the VRRP virtual router device.

Figure 1. Networking of Active-Active VRRP



Procedure

Switch A

Step1 Configure VLAN.

admin@SwitchA# set vlans vlan-id 100

admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100

admin@SwitchA# set l3-interface vlan-interface vlan100 address 192.168.1.1 prefix-length 24

admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchA#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Enable the Active-Active VRRP function.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 load-balance disable false

By default, the Active-Active VRRP function is enabled.

Step6 (Optional) Configure the interval for sending VRRP Advertisement packets.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 interval 1

By default, the value is one second.

Step7 Configure a virtual IP address for the VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5

Step8 (Optional) Configure VRRP preemptive mode.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 preempt enable true

By default, the device uses the preemptive mode.

Step9 (Optional) Configure the interval of updating the virtual MAC.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 load-balance virtual-MAC time-interval 120

By default, the value is 120s.

Step10 (Optional) Configure the priority of the device in a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 priority 250

Step11 Commit the configuration.

admin@SwitchA# commit

Switch B

Step1 Configure VLAN.

admin@SwitchB# set vlans vlan-id 100

admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 100

admin@SwitchB# set l3-interface vlan-interface vlan100 address 192.168.1.2 prefix-length 24

admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchB#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Enable the Active-Active VRRP function.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 load-balance disable false

By default, the Active-Active VRRP function is enabled.

Step6 (Optional) Configure the interval of sending VRRP Advertisement packets.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 interval 1

By default, the value is one second.

Step7 Configure a virtual IP address for the VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5

Step8 (Optional) Configure VRRP preemptive mode.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 preempt enable true

By default, the device uses the preemptive mode.

Step9 (Optional) Configure the interval of updating the virtual MAC.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 load-balance virtual-MAC time-interval 120

By default, the value is 120s.

Step10 (Optional) Configure the priority of the device in a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 priority 100

Step11 Commit the configuration.

admin@SwitchB# commit

Verify the Configuration

- After the configuration is complete, run **run show vrrp** command to view the configuration information of VRRP group. The result of show command on master is as follows.

```
admin@SwitchA# run show vrrp
Interface:                    vlan100
VRID:                         1
Version:                      3
```

```
Load-balance:                enable
State:                       Master
Master IP:                   192.168.1.1
Virtual MAC:                 00:00:5e:00:01:01
Preempt:                     enable
Adver Interval:              4
Priority:                    250
Virtual IP:                  192.168.1.5
Auth-type:                   none
Auth-key:
```

- When showing MAC address table on the downstream switch to check the MAC address of the device, you can see the virtual MAC entries corresponding to the virtual IP address of the VRRP group.
- On PC1 and PC2, ping the virtual IP address 192.168.1.5 to check the connectivity with the devices of VRRP group.

Example for Configuring Active-Active VRRPv3 for IPv6

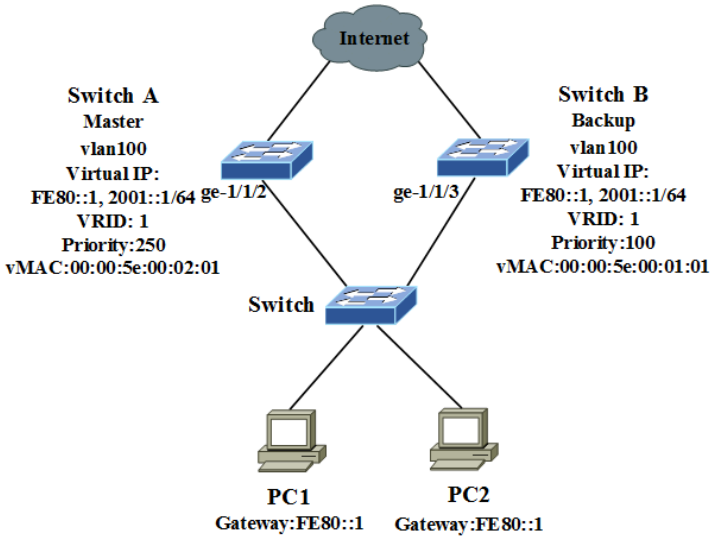
- Networking Requirements
- Procedure
  - Switch A
  - Switch B
- Verify the Configuration

Networking Requirements

Figure 1 below depicts an IPv6 network. Switch connects to the internet through gateway switches Switch A and Switch B. To ensure nonstop service availability, a VRRP group in Active-Active mode needs to be configured on Switch A and Switch B.

- Configure the VRRP router ID as 1, Switch A is the master and Switch B is the backup switch of VRRP group.
- Configure the virtual IPv6 address as 2001::1/64 and link-local address FE80::1, virtual MAC on master switch is 00:00:5e:00:02:01 and 00:00:5e:00:01:01 on the backup switch.

Figure 1. Networking of Active-Active VRRPv3 for IPv6



Procedure

Switch A

Step1 Configure VLAN.

admin@SwitchA# set vlans vlan-id 100

admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100

admin@SwitchA# set l3-interface vlan-interface vlan100 address 2001::2 prefix-length 64

admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchA#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Enable the Active-Active VRRP function.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 load-balance disable false

By default, the Active-Active VRRP function is enabled.

Step6 (Optional) Configure the interval for sending VRRPv3 advertisement packets.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 interval 1

By default, the value is one second.

Step7 Configure virtual IPv6 addresses for the VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 ip 2001::1

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 ip FE80::1

Step8 (Optional) Configure VRRP preemptive mode.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 preempt enable true

By default, the preemptive mode is enabled.

Step9 (Optional) Configure the interval of updating the virtual MAC.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 load-balance virtual-MAC time-interval 120

By default, the value is 120s.

Step10 Configure the priority of the device in a VRRP group.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 priority 250

Step11 (Optional) Enable accept mode.

admin@SwitchA# set protocols vrrp interface vlan100 vrid 1 accept disable false

Step12 Commit the configuration.

admin@SwitchA# commit

Switch B

Step1 Configure VLAN.

admin@SwitchB# set vlans vlan-id 100

admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 100

admin@SwitchB# set l3-interface vlan-interface vlan100 address 2001::3 prefix-length 64

admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100

Step2 Create a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1

Step3 Configure the VRRP version number to v3.

admin@SwitchB#set protocols vrrp interface vlan100 vrid 1 version 3

By default, the system uses VRRPv2.

Step4 Enable the VRRP function.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 disable false

By default, the VRRP function is enabled.

Step5 Enable the Active-Active VRRP function.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 load-balance disable false

By default, the Active-Active VRRP function is enabled.

Step6 (Optional) Configure the interval of sending VRRPv3 advertisement packets.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 interval 1

By default, the value is one second.

Step7 Configure virtual IPv6 addresses for the VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 ip 2001::1

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 ip FE80::1

Step8 (Optional) Configure VRRP preemptive mode.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 preempt enable true

By default, the preemptive mode is enabled.

Step9 (Optional) Configure the interval of updating the virtual MAC.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 load-balance virtual-MAC time-interval 120

By default, the value is 120s.

Step10 Configure the priority of the device in a VRRP group.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 priority 100

Step11 (Optional) Enable accept mode.

admin@SwitchB# set protocols vrrp interface vlan100 vrid 1 accept disable false

Step12 Commit the configuration.

admin@SwitchB# commit

Verify the Configuration

- After the configuration is completed, run **run show vrrp** command to view the configuration information of VRRP group. The result of show command on master is as follows.

```
admin@SwitchA# run show vrrp
Interface:                    vlan100
VRID:                         1
Version:                      2
Load-balance:                 enable
State:                        Master
Master IP:                    2001::2
Virtual MAC:                  00:00:5e:00:02:01
Preempt:                      enable
Adver Interval:               4
Priority:                     250
Virtual IP:                   2001::1, FE80::1
Auth-type:                    none
Auth-key:
```

- When showing MAC address table on the downstream switch to check the MAC address of the device, you will see the virtual MAC entries corresponding to the virtual IP address of the VRRP group.
- On PC1 and PC2, ping the virtual IP address FE80::1 to check the connectivity with the devices of VRRP group.

IPv4/IPv6 BGP Configuration

This section describes how to use Border Gateway Protocol (BGP) protocol.

NOTE:
- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.
- BGP protocol supports VRF.

- BGP Introduction
- BGP Regular Expressions
- Basic BGP Configuration
- Configuring BGP Security
- Configuring a BGP Route Reflector
- Configuring BGP Timers
- Configuring BGP Route Aggregation
- Configuring BGP Dynamic Neighbors
- Configuring eBGP Multihop
- Configuring Removing and Replacing Private ASNs from the AS Path
- Configuring BGP Multipath
- Configuring ebgp-requires-policy
- Enable BGP Read-only Mode
- Configuring Route Maps for Route Updates
- BGP Unnumbered
  - Overview of BGP Unnumbered
  - Example for Configuring Basic BGP Unnumbered
  - Example for Configuring BGP Unnumbered EVPN Fabric
- Configuring BGP Attribute
  - Configuring the AS_Path Attribute
  - Configuring the BGP Community Attribute
  - Configuring the MED Attribute
  - Configuring the Next_Hop Attribute
- Configuration Examples
  - Example for Configuring Basic BGP Functions
  - Example for Configuring a BGP Route Reflector
  - Example for Configuring BGP Load Balancing

BGP Introduction

BGP is a path vector protocol used to carry routing information between autonomous systems.The term path vector comes from the fact that BGP routing information carries a sequence of AS numbers that identifies the path of AS's that a network prefix has traversed. The path information associated with the prefix is used to enable loop prevention.

BGP uses TCP as its transport protocol (port 179). This ensures that all the transport reliability (such as retransmission) is taken care of by TCP and does not need to be implemented in BGP, thereby simplifying the complexity associated with designing reliability into the protocol itself.

> **NOTE:**
> BGP protocol supports VRF.

BGP Speaker and BGP Peers

Routers that run a BGP routing process are often referred to as BGP speakers.Two BGP speakers that form a TCP connection between one another for the purpose of exchanging routing information, are referred to as neighbors or peers. Peer routers exchange open messages to determine the connection parameters.These messages are used to communicate values such as the BGP speaker's version number.

Gracefully Shutdown

BGP also provides a mechanism to gracefully close a connection with a peer. In other words, in the event of a disagreement between the peers, be it resultant of configuration, incompatibility, operator intervention, or other circumstances, a NOTIFICATION error message is sent, and the peer connection does not get established or is torn down if it's already established. The benefit of this mechanism is that both peers understand that the connection could not be established or maintained and do not waste resources that would otherwise be required to maintain or blindly reattempt to establish the connection. The graceful close mechanism simply ensures that all outstanding messages, primarily NOTIFICATION error messages, are delivered before the TCP session is closed.

BGP Session Establishment

Initially, when a BGP session is established between a set of BGP speakers, all candidate BGP routes are exchanged. After the session has been established and the initial route exchange has occurred, only incremental updates are sent as network information changes.

Routes are advertised between a pair of BGP routers in UPDATE messages. The UPDATE message contains, among other things, a list of <length, prefix> tuples that indicate the list of destinations that can be reached via a BGP speaker. The UPDATE message also contains the path attributes, which include such information as the degree of preference for a particular route and the list of AS's that the route has traversed.

In the event that a route becomes unreachable, a BGP speaker informs its neighbors by withdrawing the invalid route. Withdrawn routes are part of the UPDATE message. These routes are no longer available for use. If information associated with a route has changed or a new path for the same prefix has been selected, a withdrawal is not required; it is enough to just advertise a replacement route.

KEEPALIVE Message

If no routing changes occur, the routers exchange only KEEPALIVE packets.

KEEPALIVE messages are sent periodically between BGP neighbors to ensure that the connection is kept alive. KEEPALIVE packets (19 bytes each) should not cause any strain on the router CPU or link bandwidth because they consume a minimal amount of bandwidth.

BGP Attributes

BGP attributes of the routes can be used in route selection and load balancing. The following describes common BGP route attributes:

- **Origin**

  The Origin attribute defines the origin of a route and marks the path of a BGP route. The Origin attribute is classified into three types:

  - IGP

    A route with IGP as the Origin attribute is of the highest priority. The Origin attribute of the routes imported into a BGP routing table using the **set protocols bgp** [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network <***ipv4/prefixlen***> [label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]** command is IGP.

  - EGP

    A route with EGP as the Origin attribute is of the secondary highest priority. The Origin attribute of the routes obtained through EGP is EGP.

- Incomplete

  A route with Incomplete as the Origin attribute is of the lowest priority. The Origin attribute of the routes learned by other means is Incomplete. For example, the Origin attribute of the routes imported by BGP using the **set protocols bgp** [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|static|table <***table-number***>**} [**metric** <*metric-number*>|**route-map** <*route-map*>] command is Incomplete.

- **AS_Path**

  The AS_Path attribute records all the ASs that a route passes through from the source to the destination in the vector order. To prevent inter-AS routing loops, a BGP device does not receive the routes of which the AS_Path list contains the local AS number.

  When a BGP speaker advertises an imported route:

  - If the route is advertised to EBGP peers, the BGP speaker creates an AS_Path list containing the local AS number in an Update message.
  - If the route is advertised to IBGP peers, the BGP speaker creates an empty AS_Path list in an Update message.

  When a BGP speaker advertises a route learned in the Update message sent by another BGP speaker:

  - If the route is advertised to EBGP peers, the BGP speaker adds the local AS number to the leftmost of the AS_Path list. According to the AS_Path list, the BGP speaker that receives the route can learn about the ASs through which the route passes to reach the destination. The number of the AS that is nearest to the local AS is placed on the top of the AS_Path list. The other AS numbers are listed according to the sequence in which the route passes through ASs.
  - If the route is advertised to IBGP peers, the BGP speaker does not change the AS_Path attribute of the route.

- **Next_Hop**

  The Next_Hop attribute records the next hop that a route passes through. The Next_Hop attribute of BGP is different from that of an IGP because it may not be the neighbor IP address. A BGP speaker processes the Next_Hop attribute based on the following rules:

  - When advertising a route to an EBGP peer, a BGP speaker sets the Next_Hop attribute of the route to the address of the local interface through which the BGP peer relationship is established with the peer.
  - When advertising a locally originated route to an IBGP peer, the BGP speaker sets the Next_Hop attribute of the route to the address of the local interface through which the BGP peer relationship is established with the peer.
  - When advertising a route learned from an EBGP peer to an IBGP peer, the BGP speaker does not change the Next_Hop attribute of the route.

- **Local_Pref**

  The Local_Pref attribute indicates the BGP preference of a device and helps determine the optimal route when traffic leaves an AS. When a BGP device obtains multiple routes to the same destination address but with different next hops from different IBGP peers, the BGP device prefers the route with the highest Local_Pref. The Local_Pref attribute is exchanged only between IBGP peers and is not advertised to other ASs. The Local_Pref attribute can be manually configured. If no Local_Pref attribute is configured for a route, the Local_Pref attribute of the route uses the default value 100.

- **MED**

  The multi-exit discriminator (MED) attribute helps determine the optimal route when traffic enters an AS. When a BGP device obtains multiple routes to the same destination address but with different next hops from EBGP peers, the BGP device selects the route with the smallest MED value as the optimal route.

  The MED attribute is exchanged only between two neighboring ASs. The AS that receives the MED attribute does not advertise it to any other ASs. The MED attribute can be manually configured. If no MED attribute is configured for a route, the MED attribute of the route uses the default value 0.

- **Community**

  The Community attribute identifies the BGP routes with the same characteristics, simplifies the applications of routing policies, and facilitates route maintenance and management.

  The Community attribute includes self-defined community attributes and well-known community attributes. **Table 1** lists well-known community attributes.

  Table 1 Well-known community attributes

Community Attribute	Value	Description
Internet	0 (0x00000000)	A BGP device can advertise the received route with the Internet attribute to all peers.
No_Advertise	4294967042 (0xFFFFFF02)	A BGP device does not advertise the received route with the No_Advertise attribute to any peer.
No_Export	4294967041 (0xFFFFFF01)	A BGP device does not advertise the received route with the No_Export attribute to devices outside the local AS.
No_Export_Subconfed	4294967043 (0xFFFFFF03)	A BGP device does not advertise the received route with the No_Export_Subconfed attribute to devices outside the local AS or to devices outside the local sub-AS.

- **Originator_ID and Cluster_List**

  The Originator_ID attribute and Cluster_List attribute help eliminate loops in route reflector scenarios.

BGP Regular Expressions

A regular expression is a mode matching tool. You can create a matching mode based on specified rules and then match target objects based on the matching mode. A regular expression consists of 1 to 256 common characters and special characters.

- Common characters

  Common characters are used to match themselves in a string, including all upper-case and lower-case letters, digits, punctuations, underline, and special symbols. For example, a matches the letter "a" in "abc", 10 matches the digit "10" in "10.113.25.155", and @ matches the symbol "@" in "xxx@xxx.com".

- Special characters

  Special characters are a set of symbols with special meanings which are provided to flexibly create matching modes. The following special characters are supported by PICOS:

  .* Matches any single character.
  * Matches 0 or more occurrences of pattern.
  + Matches 1 or more occurrences of pattern.
  ? Match 0 or 1 occurrences of pattern.
  ^ Matches the beginning of the line.
  $ Matches the end of the line.
  _ The _ character has special meanings in BGP regular expressions. It matches to space and comma , and AS set delimiter { and } and AS confederation delimiter (and). And it also matches to the beginning of the line and the end of the line. So _ can be used for AS value boundaries match. This character technically evaluates to (^|[,{}()]|$).

> **NOTE:**
> Note that space is not supported, even if in a double quotation marks "".

Basic BGP Configuration

- Configuring a BGP Router ID
- Configuring BGP Local-AS
- Configuring External BGP Peering
- Configuring Internal BGP Peering
- Configuring a BGP Peer Group
- Configuring BGP to Import Routes
  - Redistribute Mode
  - Network Mode

For IPv6 BGP configuration, the following command must be configured to enable the IPv6 address family capability and exchange of information specific to an IPv6 address family with a BGP neighbor.
set protocols bgp [**vrf** *<vrf-name>*] **{neighbor** *<ip>***| peer-group** *<peer-group>* |**interface** *<interface>***}** {**ipv6-unicast|ipv6-labeled-unicast**} **activate true**

Configuring a BGP Router ID

The router ID should be configured first when you configure BGP. The router ID is a string similar to the IP address, and is the identifier of a BGP router in an AS. You should not change the router ID after completing the configuration. By default, the BGP router ID is not configured.

```
admin@XorPlus# set protocols bgp router-id 1.1.1.1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring BGP Local-AS

The local ASN (Autonomous System Number) should be configured when you configure BGP. An Autonomous System (AS) is a group of IP networks that are controlled by one entity, typically an Internet service provider (ISP), and that have the same routing policy. Each AS is assigned a unique AS number, which identifies an AS on a BGP network.

The AS_Path attribute records all the AS numbers that a route passes through, from the source to the destination, following the order of vectors.

```
admin@XorPlus# set protocols bgp local-as 100
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring External BGP Peering

If the AS number of the specified peer is different from the local AS number during the configuration of BGP peers, an EBGP peer is configured. To establish point-to-point connections between peer autonomous systems, configure a BGP session on each interface of a point-to-point link. Generally, such sessions are made at network exit points with neighboring hosts outside the AS.

```
admin@XorPlus# set protocols bgp local-as 100
admin@XorPlus# set protocols bgp neighbor 192.168.49.1 remote-as 200
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Internal BGP Peering

If the AS number of the specified peer is the same as the local AS number during the configuration of BGP peers, an IBGP peer is configured.

```
admin@XorPlus# set protocols bgp local-as 100
admin@XorPlus# set protocols bgp neighbor 192.168.49.1 remote-as 100
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring a BGP Peer Group

A large BGP network has a large number of peers. It is difficult to configure and maintain these peers. You can add the BGP peers with the same configurations to a BGP peer group and then configure the BGP peers in batches. This simplifies peer management and improves route advertisement efficiency.

> **NOTE:**
>
> - If a BGP configuration exists on a peer and its peer group, the BGP configuration on the peer takes precedence over the configuration on the peer group.
> - If the peer you want to add to a group already exists in the BGP configuration, delete it first, than add it to the peer group.

The following example commands create a peer group called Leaf1 that includes two external peers.

```
admin@XorPlus# set protocols bgp peer-group Leaf1
admin@XorPlus# set protocols bgp peer-group Leaf1 remote-as external
admin@XorPlus# set protocols bgp neighbor 10.10.0.1 peer-group Leaf1
admin@XorPlus# set protocols bgp neighbor 10.10.0.12 peer-group Leaf1
admin@XorPlus# commit
```

Configuring BGP to Import Routes

BGP cannot discover routes and needs to import routes such as IGP routes into BGP routing tables so that the imported routes can be transmitted within an AS or between ASs. BGP imports routes in either redistribute or network mode.

> **NOTE:**
> If you do not want to control the route exchanging via use BGP policies, you need to disable feature *ebgp-requires-policy* manually, or the route cannot be correctly exchanged. For details about *ebgp-requires-policy*, see page Configuring ebgp-requires-policy.

Redistribute Mode

In redistribute mode, BGP imports IGP routes, including RIP, OSPF, and IS-IS routes, into BGP routing tables based on protocol type. To ensure the validity of imported IGP routes, BGP can also import static routes and direct routes in redistribute mode.

Use the following command to configure to import BGP route:

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|static|table <***table-number***>**} [**metric** <*metric-number*>|**route-map** <*route-map*>]

Network Mode

In network mode, BGP imports the routes in the IP routing table one by one to BGP routing tables. The network mode is more accurate than the redistribute mode. The ORIGIN attribute of BGP routes advertised in this way is IGP.

Use the following commands to configure BGP to statically add routes in the IP routing table to the BGP routing table and advertise these routes to peers.

Apply the specified route policy or a route label to control network advertisements with the following command:

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network <***ipv4/prefixlen***> [label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]**

The network mode command is used to import exactly-matching routes. The mask length as configured in the network statement must match the mask length of prefixes in the routing table. This means that the specified network must be available and active in the local IP routing table.

Configuring BGP Security

- Configuring MD5 Authentication
- Configuring TTL Security Hop Count

Configuring MD5 Authentication

BGP uses TCP as the transmission protocol, and considers a packet valid as long as the source address, destination address, source port, destination port, and TCP sequence number of the packet are correct. However, most parameters in a packet may be easily obtained by attackers. To protect BGP from attacks, MD5 authentication can be used between BGP peers to reduce the possibility of attacks. The MD5 algorithm is easy to configure, generates a single password that needs to be manually changed.

```
admin@XorPlus# set protocols bgp neighbor 192.10.10.2 password picos12345
admin@XorPlus# commit
```

Configuring TTL Security Hop Count

This feature enables BGP to establish connection with external peers residing on networks that are not directly connected. By enabling this feature, the received TTL from a BGP peer is compared with the difference "255 - hop-count". BGP messages coming with a TTL less than this value are not accepted. BGP peering will not be established if the TTL in the session establishment is received with a lower value. Also, by enabling this feature the router will send BGP packets with TTL value of 255 to the neighbor. For a neighbor, either TTL security or ebgp-multihop can be configured, not both together. If there are multiple paths to reach the node, then the hop count should be configured considering the longest route.

```
admin@XorPlus# set protocols bgp neighbor 192.10.10.2 ttl-security hops 200
admin@XorPlus# commit
```

Configuring a BGP Route Reflector

To ensure the connectivity between IBGP peers within an AS, you need to establish full-mesh connections between the IBGP peers. When there are many IBGP peers, it is costly to establish a fully-meshed network. A route reflector (RR) can solve this problem.

A cluster ID can help prevent routing loops between multiple RRs within a cluster and between clusters. When a cluster has multiple RRs, the same cluster ID must be configured for all the RRs within the cluster.

Enabling Route Reflector

The following example configures the local device Switch1 as the route reflector and the peer Switch2 as the client of the route reflector. No configuration is required on the client.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast route-reflector-client
admin@XorPlus# commit
```

Configuring Cluster ID

The following example configures a cluster ID for the RR. By default, each RR uses its router ID as the cluster ID.

```
admin@XorPlus# set protocols bgp cluster-id 100.100.100.100
admin@XorPlus# commit
```

Configuring BGP Timers

When deploying BGP, there are several timers can be configured.

- Configuring BGP Keepalive and Hold Timers
- Configuring a BGP Reconnect Timer
- Configuring a Advertisement Interval
- Configuring the Global BGP Timers

Configuring BGP Keepalive and Hold Timers

Keepalive messages are used by BGP to maintain peer relationships.

- If short Keepalive time and holdtime are set, BGP can detect a link fault quickly. This speeds up BGP network convergence, but increases the number of Keepalive messages on the network and loads of devices, and consumes more network bandwidth resources.
- If long Keepalive time and holdtime are set, the number of Keepalive messages on the network is reduced, loads of devices are reduced, and fewer network bandwidth are consumed. If the Keepalive time is too long, BGP is unable to detect link status changes in a timely manner. This is unhelpful for implementing rapid BGP network convergence and may cause many packets to be lost.

Keepalive and hold timers can be configured either for a specific peer or peer group, and the configurations for a specific peer take precedence over those for the peer group of this peer.

The following example commands set the keepalive interval to 10 seconds and the hold time to 30 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers keepalive 10
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers holdtime 30
admin@XorPlus# commit
```

Configuring a BGP Reconnect Timer

After BGP initiates a TCP connection, the Reconnect timer will be stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the Reconnect timer expires.

- Setting a short Reconnect interval reduces the period BGP waits between attempts to establish a TCP connection. This speeds up the establishment of the TCP connection.
- Setting a long Reconnect interval suppresses routing flapping caused by peer relationship flapping.

A Reconnect timer can be configured either for a specific peer or peer group, and the configurations for a specific peer take precedence over those for the peer group of this peer.

This example sets the Re-connection value to 30 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers connect 30
admin@XorPlus# commit
```

Configuring a Advertisement Interval

BGP does not periodically update a routing table. When BGP routes change, BGP updates the changed BGP routes in the BGP routing table by sending Update messages.

- If a short Update message interval is set, BGP can fast detect route changes. This speeds up BGP network convergence, but increases the number of Update messages on the network and loads of devices, and consumes more network bandwidth resources.
- If a long Update message interval is set, the number of Update messages on the network is reduced, loads of devices are reduced, and fewer network bandwidth are consumed. This avoids network flapping. If the Update message interval is too long, BGP is unable to detect route changes in a timely manner. This is unhelpful for implementing rapid BGP network convergence and may cause many packets to be lost.

When routes change, the switch sends routing updates to notify its peers. If a route changes frequently, the **set protocols bgp** [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} advertisement-interval** <*advert-interval*> command can be used to adjust the interval at which Update packets are sent for changes of this route. This frees the switch from sending Update packets for every route change.

The following example commands set the advertisement interval to 5 seconds:

```
admin@XorPlus# set protocols bgp neighbor 1.1.1.1 advertisement-interval 5
admin@XorPlus# commit
```

Configuring the Global BGP Timers

In addition to the timers configured for a specific neighbor or a peer goup described above, BGP also supports to configure global timers for all the BGP neighbors.

The following example commands set the keepalive interval to 10 seconds and the hold time to 30 seconds globally for all the BGP neighbors.

```
admin@XorPlus# set protocols bgp timers keepalive 10
admin@XorPlus# set protocols bgp timers holdtime 30
```

```
admin@XorPlus# commit
```

Configuring BGP Route Aggregation

Route aggregation is a mechanism that combines multiple routes into one route. This mechanism allows a BGP device to advertise only the summarized route but not all the specific routes to peers, therefore reducing the size of the BGP routing table. If the aggregated route flaps, the network is not affected, so network stability is improved.

To prevent routing loops caused by route summarization, BGP uses the AS_Set attribute. The AS_Set attribute is an unordered set of all ASs that a route passes through. When the summarized route enters an AS in the AS_Set attribute again, BGP finds that the local AS number has been recorded in the AS_Set attribute of the route and discards this route to prevent a routing loop.

The following example command aggregates a range of addresses, such as 10.10.1.0/24, 10.10.2.0/24, 10.10.3.0/24 into the single prefix 10.10.0.0/16.

```
admin@Xorplus# set protocols bgp ipv4-unicast aggregate-address 10.10.0.0/16
admin@Xorplus# commit
```

Configuring BGP Dynamic Neighbors

BGP dynamic neighbors are established by creating a listen range and accepting incoming connections from neighbors in that address range.

The BGP command **set protocols bgp** [**vrf** <*vrf-name*>] **listen range {**<*ipv4/prefixlen*>|<*ipv6/prefixlen*>**} peer-group** <*peer-group*> specifies a range of IPv4 addresses from which the switch will accept incoming dynamic BGP peering requests, and creates the named dynamic peer group to which those peers belong. Dynamic BGP neighbors are peers which have not been manually established, but are accepted into a dynamic peer group when the switch receives a peering request from them.

Dynamic peers cannot be configured individually, but inherit any configuration that is applied to the peer group to which they belong. In larger BGP networks, implementing BGP dynamic neighbors can reduce the amount and complexity of CLI configuration and save CPU and memory usage. Only IPv4 peering is supported. Peering relationships with dynamic peers are terminated if the peer group is deleted.

The following example commands create the peer group Leaf1 and configure BGP peering to remote neighbors within the address range 10.10.10.0/31. The **set protocols bgp listen limit** command limits the number of dynamic peers. The default value is 100.

```
admin@XorPlus# set protocols bgp peer-group Leaf1
admin@XorPlus# set protocols bgp peer-group Leaf1 remote-as external
admin@XorPlus# set protocols bgp listen range 10.10.10.0/31 peer-group Leaf1
admin@XorPlus# set protocols bgp listen limit 10
admin@XorPlus# commit
```

Configuring eBGP Multihop

External BGP peering sessions are configured to allow BGP peers from different autonomous systems to exchange routing updates. By design, a BGP routing process expects eBGP peers to be directly connected. When the neighbor is not directly connected, then we can enable eBGP Multihop function to allow the session to be established.

In this example, BGP is configured to allow connections to or from neighbor 192.168.1.1, which resides on a network that is not directly connected.

```
admin@XorPlus# set protocols bgp neighbor 192.168.1.1 remote-as external
admin@XorPlus# set protocols bgp neighbor 192.168.1.1 ebgp-multihop maximum-hop 5
admin@XorPlus# commit
```

Configuring Removing and Replacing Private ASNs from the AS Path

External BGP requires that globally unique AS numbers be used when routing to the global Internet. Using private AS numbers (64512 to 65535) would prevent access to the global Internet. This feature allows routers that belong to a private AS to access the global Internet. A network administrator configures the routers to remove private AS numbers from the AS path contained in outgoing update messages and optionally, to replace those numbers with the ASN of the local router, so that the AS Path length remains unchanged.

The **replace-as** keyword is available to replace the private AS numbers being removed from the path with the local AS number, thereby retaining the same AS path length.

This example removes all the private AS numbers from the AS path in outgoing eBGP updates and replaces them with the public AS number of the local router.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast remove-private-as all replace-as
admin@XorPlus# commit
```

Configuring BGP Multipath

On a large network, there may be multiple valid BGP routes to the same destination. A switch will select and add the optimal BGP route to its routing table for traffic forwarding and advertises this route to its peers. This, however, will result in uneven load balancing of many traffic. Configuring BGP load balancing can enable the switch to add these multiple equal-cost BGP routes to its routing table, implementing traffic load balancing and reducing network congestion. After BGP load balancing is configured, the switch will still select the optimal route among the multiple routes and advertise only this route to its peers.

In PICOS system, the BGP multipath option is enabled so that the switch can install multiple equal-cost BGP paths to the forwarding table and load balance traffic across multiple links. You can change the number of paths allowed, according to your needs.

The example commands change the maximum number of paths to 12. You can set a value between 1 and 32. 1 disables the BGP multipath option.

```
admin@XorPlus# set protocols bgp ipv4-unicast multipath ibgp maximum-paths 12
admin@XorPlus# commit
```

For paths to be consider equal, they must have the same routes attributes, such as weight, local preference, origin and AS_Path attributes are the same. If any of these attribues are different, BGP multipath will NOT take effect.

But in a special case, we can use the **set protocols bgp**[***vrf***<*vrf-name*>]**bestpath as-path multipath-relax [as-set|no-as-set]** command to configure Border Gateway Protocol (BGP) to treat two BGP routes as equal cost even if their AS-paths differ, as long as their AS-path lengths and other relevant attributes are the same. This allows routes with different AS-paths to be programmed into the forwarding table as equal cost multipath routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

```
admin@XorPlus# set protocols bgp bestpath as-path multipath-relax
admin@XorPlus# commit
```

Configuring ebgp-requires-policy

Users can use the command **set protocols bgp** [**vrf** <*vrf-name*>] **ebgp-requires-policy** <**true | false**> to determine whether or not EBGP will exchange routes with peers based on a policy. Choosing **true** requires filters (filter-list, prefix-list or route-map defined) for every eBGP session.

Consider creating appropriate route maps and using them rather than disabling the policy check. As a best practice, using policies is a more secure behavior and can prevent unintended routes from being exchanged. Function **ebgp-requires-policy** is introduced and enabled by default.

With this command enabled, EBGP will not exchange routes with a neighbor unless there is a route map configured on the address family neighbor entry which matches and permits the routes inbound and outbound. That is, without an incoming filter, no routes will be accepted. Similarly, without an outgoing filter, no routes will be announced.

The following commands configure a BGP route policy “rm1” and enables ebgp-requires-policy to filter the incoming routes based on this policy.

```
admin@Xorplus# set routing prefix-list ipv4-family plist1 permit prefix 13.13.13.0/24
admin@Xorplus# set routing route-map rm1 order 1 matching-policy permit
admin@Xorplus# set routing route-map rm1 order 1 match ipv4-addr address prefix-list plist1
admin@Xorplus# set protocols bgp neighbor 192.168.170.1 ipv4-unicast in route-map rm1
admin@Xorplus# set protocols bgp ebgp-requires-policy true
admin@Xorplus# commit
```

NOTE:
If you do not want to control the route exchange via the use of BGP policies, you need to disable this feature manually otherwise the routes will not be exchanged properly.

When **ebgp-requires-policy** is enabled but the incoming or outgoing filter is missing, then the incoming route would be discarded and the outgoing route would not be allowed to advertise.

Additionally, a **run show bgp neighbor** command output would indicate in the *For address family:* section that *updates discarded due to missing policy* as shown below:

```
admin@Xorplus# run show bgp neighbor
...
For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
...
For address family: IPv6 Unicast
  Update group 2, subgroup 2
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
```

Enable BGP Read-only Mode

When the router starts to receive the prefix at the time of initialization, the path selection process has been run in advance, which will cause the best path to keep changing, so that multiple updates of the same prefix will be sent, which is inefficient.

Enable read-only mode to reduce CPU and network usage when restarting the BGP process. When applicable, read-only mode would begin as soon as the first peer reaches Established status and a timer for maximum delay seconds is started. During this mode BGP doesn't run any best-path or generate any updates to its peers. This mode continues until either of the following two conditions are met:
1. All the configured peers, except the shutdown peers, have sent explicit EOR (End-Of-RIB) or an implicit- EOR. The first keep-alive after BGP has reached Established is considered an implicit-EOR. If the establish-wait optional value is given, then BGP will wait for peers to reach established from the beginning of the update-delay till the establish-wait period is over, i.e. the minimum set of established peers for which EOR is expected would be peers established during the establish-wait window, not necessarily all the configured neighbors.
2. maximum delay period is over.
On hitting any of the above two conditions, BGP resumes the decision process and generates updates to its peers.
Default maximum delay is 0, i.e. the read-only mode is disabled by default.

Note that the establish-wait setting is optional; however, if specified, it must be shorter than the maximum delay timer.

The following example commands enable read-only mode by setting the maximum delay timer to 500 seconds and the establish-wait timer to 90 seconds.

```
admin@XorPlus# set protocols bgp update-delay delay 500
admin@XorPlus# set protocols bgp update-delay establish-wait 90
admin@XorPlus# commit
```

Configuring Route Maps for Route Updates

You can apply **route maps** in BGP in one of two ways:

- Filter routes from BGP into Zebra
- Filter routes from Zebra into the Linux kernel

Filter Routes from BGP into Zebra

You can apply a route map on route updates from BGP to Zebra. All the applicable match operations are allowed, such as match on prefix, next hop, communities, and so on. Set operations are limited to metric and next hop only. Applying a route map on route updates from BGP to Zebra does not affect the BGP internal RIB.
Both IPv4 and IPv6 address families are supported. Route maps work on multi-paths; however, the metric setting is based on the best path only.

The following example command applies a route map called routemap1 to filter route updates from BGP into Zebra:

```
admin@XorPlus# set protocols bgp ipv4-unicast table-map routemap1
admin@XorPlus# commit
```

Filter Routes from Zebra into the Linux Kernel

The following example commands apply a route map called routemap1 to filter route updates from Zebra into the Linux kernel:

```
admin@XorPlus# set routing protocol bgp route-map routemap1
admin@XorPlus# commit
```

BGP Unnumbered

- Overview of BGP Unnumbered
- Example for Configuring Basic BGP Unnumbered
- Example for Configuring BGP Unnumbered EVPN Fabric

Overview of BGP Unnumbered

In a traditional Layer 3 network, an IP address should be assigned to each interface to provide connectivity from one link endpoint to another. But in the data center network, with a large number of spine and leaf devices and the number of interfaces interconnecting them could be very large. This leads to a sharp increase in the number of IP addresses required. Such large networks can consume a lot of IP addresses, where each peer requires a separate IP address.

BGP unnumbered is very useful in this kind of scenarios. BGP unnumbered interface is a BGP interface that does not need to specify a unique IP address, it uses the IPv6 link-local address, which is assigned automatically to each interface. BGP unnumbered works by using the Extended Next Hop Encoding (ENHE) as defined in RFC 5549, which provides a way to advertise an IPv4 route with an IPv6 next-hop. The IPv6 next-hop is resolved by using the IPv6 Neighbor Discovery (ND) process. Prior to RFC 5549, an IPv4 route could only be advertised with an IPv4 next-hop.

For BGP unnumbered, the next-hop address for each prefix is an IPv6 link-local address, which is assigned automatically to each interface. Using the IPv6 link-local address as a next-hop instead of an IPv4 unicast address, BGP unnumbered saves you from having to configure IPv4 addresses on each interface.

NOTEs:

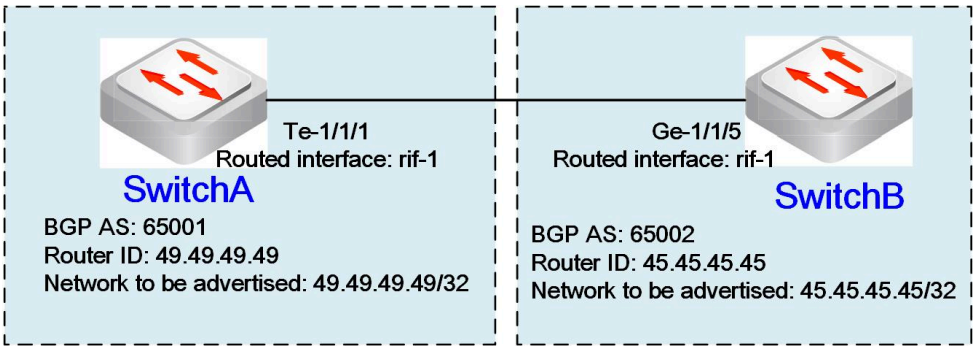
BGP unnumbered can only be used on two switches with point-to-point connection.

Example for Configuring Basic BGP Unnumbered

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
- Verify the Configuration

Networking Requirements

Figure 1. BGP Unnumbered Configuration Example



As shown in **Figure 1**, Switch A and Switch B are BGP peers. An EBGP connection is established between Switch A and Switch B. To save IP addresses, BGP unnumbered can be configured between Switch A and Switch B. In this example, routed interfaces are configured for the use of BGP unnumbered interface.

The only difference between a BGP unnumbered configuration and the BGP numbered configuration is that the BGP neighbor is specified as an interface instead of an IP address. The interface between the two peers does not need to have an IP address configured on each side.

> **NOTE:**
>
> The ebgp-requires-policy function needs to be disabled in EBGP, no need in IBGP.

Procedure

Switch A

Step 1 Enable te-1/1/1 as a routed interface and configure the interface name as rif-1.

```
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 routed-interface enable true
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 routed-interface name rif-1
admin@SwitchA# set vlans reserved-vlan 80-90
admin@SwitchA# set l3-interface routed-interface rif-1
```

Step 2 Configure EBGP and disable ebgp-requires-policy policy.

```
admin@SwitchA# set protocols bgp local-as 65001
admin@SwitchA# set protocols bgp router-id 49.49.49.49
admin@SwitchA# set protocols bgp interface rif-1 remote-as 65002
admin@SwitchA# set protocols bgp interface rif-1 ipv6-unicast activate true
admin@SwitchA# set protocols bgp interface rif-1 capability extended-nexthop
admin@SwitchA# set protocols bgp ebgp-requires-policy false
```

Step 3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step 4 Advertise the host subnets through BGP.

```
admin@SwitchA# set protocols bgp ipv4-unicast network 49.49.49.49/32
```

Step 5 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step 1 Enable ge-1/1/5 as a routed interface and configure interface name as rif-1.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/5 routed-interface enable true
admin@SwitchB# set interface gigabit-ethernet ge-1/1/5 routed-interface name rif-1
admin@SwitchB# set vlans reserved-vlan 80-90
admin@SwitchB# set l3-interface routed-interface rif-1
```

Step 2 Configure EBGP and disable ebgp-requires-policy policy.

```
admin@SwitchB# set protocols bgp local-as 65002
admin@SwitchB# set protocols bgp router-id 45.45.45.45
admin@SwitchB# set protocols bgp interface rif-1 remote-as 65001
admin@SwitchB# set protocols bgp interface rif-1 ipv6-unicast activate true
admin@SwitchB# set protocols bgp interface rif-1 capability extended-nexthop
admin@SwitchB# set protocols bgp ebgp-requires-policy false
```

Step 3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step 4 Advertise the host subnets through BGP.

```
admin@SwitchB# set protocols bgp ipv4-unicast network 45.45.45.45/32
```

Step 5 Commit the configuration.

```
admin@SwitchB# commit
```

Verify the Configuration

- Check the BGP neighbor by running the following command.

```
admin@SwitchA# run show bgp neighbor
BGP neighbor on rif-1: fe80::1a5a:5810:83c:42a1, remote AS 65002, local AS 65001, external link
Hostname: SwitchB
  BGP version 4, remote router ID 45.45.45.45, local router ID 49.49.49.49
  BGP state = Established, up for 00:03:38
  Last read 00:00:38, Last write 00:00:38
  Hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Extended Message: advertised and received
    AddPath:
      IPv4 Unicast: RX advertised IPv4 Unicast and received
      IPv6 Unicast: RX advertised IPv6 Unicast and received
    Extended nexthop: advertised and received
      Address families by peer:
                IPv4 Unicast
    Route refresh: advertised and received(old & new)
    Enhanced Route Refresh: advertised and received
    Address Family IPv4 Unicast: advertised and received
    Address Family IPv6 Unicast: advertised and received
    Hostname Capability: advertised (name: 49sw,domain name: n/a) received (name: 45sw,domain name: n/a)
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families by peer:
        none
  Graceful restart information:
    End-of-RIB send: IPv4 Unicast, IPv6 Unicast
    End-of-RIB received: IPv4 Unicast, IPv6 Unicast
    Local GR Mode: Helper*
    Remote GR Mode: Helper
```

```
    R bit: True
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 120
    IPv4 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: No
      End-of-RIB received: Yes
      Timers:
        Configured Stale Path Time(sec): 360
    IPv6 Unicast:
      F bit: False
      End-of-RIB sent: Yes
      End-of-RIB sent after update: Yes
      End-of-RIB received: Yes
      Timers:
        Configured Stale Path Time(sec): 360
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  3          2
    Notifications:          0          2
    Updates:                9          9
    Keepalives:             5          5
    Route Refresh:          0          0
    Capability:             0          0
    Total:                 17         18
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Update group 5, subgroup 5
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  1 accepted prefixes

 For address family: IPv6 Unicast
  Update group 6, subgroup 6
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 1; dropped 0
  Last reset 00:03:41,  No AFI/SAFI activated for peer
Local host: fe80::1a5a:5820:61f:63a1, Local port: 179
Foreign host: fe80::1a5a:5810:83c:42a1, Foreign port: 57988
Nexthop local: fe80::1a5a:5820:61f:63a1
BGP connection: shared network
BGP Connect Retry Timer in Seconds: 120
Estimated round trip time: 2 ms
Read thread: on  Write thread: on  FD used: 25
```

- After completing the configuration, check BGP route on the switches.

```
admin@SwitchA# run show route bgp
RIB entry for bgp
=================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, A - Babel, F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 45.45.45.45/32 [20/0] via fe80::1a5a:5810:83c:42a1, rif-1, weight 1, 02:03:58
```

- Show the brief information for BGP.

```
admin@SwitchA# run show bgp
```

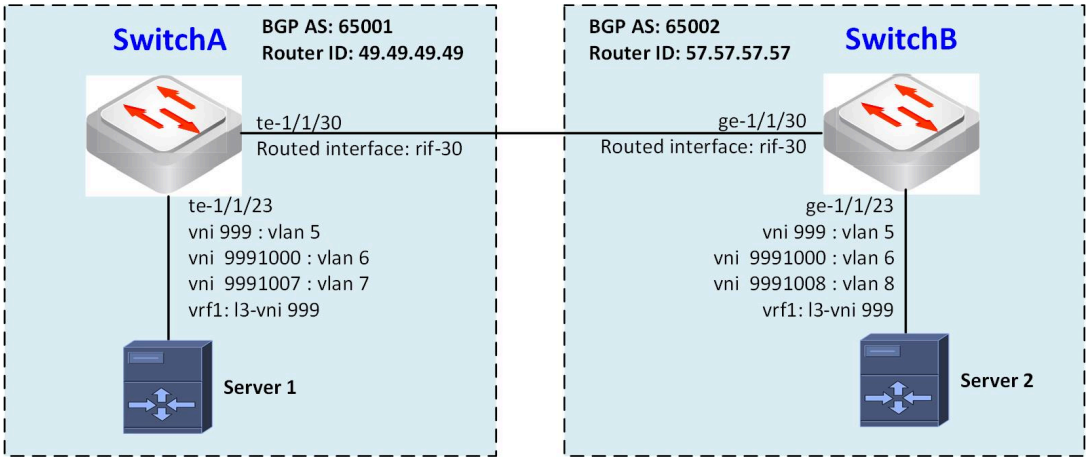
```
show bgp ipv4 unicast
=====================
BGP table version is 10, local router ID is 49.49.49.49, vrf id 0
Default local pref 100, local AS 65001
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop            Metric LocPrf Weight Path
*> 45.45.45.45/32   rif-1                       0             0 65002 i

Displayed 1 routes and 1 total paths

show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

Example for Configuring BGP Unnumbered EVPN Fabric

- Networking Requirements
  - Figure 1. BGP Unnumbered EVPN Fabric Configuration Example
- Procedure
  - Switch A
  - Switch B
- Verify the Configuration

Networking Requirements

Figure 1. BGP Unnumbered EVPN Fabric Configuration Example



As shown in **Figure 1**, this example configures BGP unnumbered on EVPN VTEP devices Switch A and Switch B. An eBGP connection is established between Switch A and Switch B.

In this example, routed interfaces are configured f to be used as BGP unnumbered interfaces for EVPN underlay fabric.

The only difference between a BGP unnumbered configuration and the BGP numbered configuration is that the BGP neighbor is specified as an interface instead of an IP address. The interfaces connecting the two peers do not need to have IP addresses configured on each side.

> **NOTE:**
>
> The ebgp-requires-policy function needs to be disabled in EBGP, no need in IBGP.

Procedure

Switch A

Step 1 Configure physical interfaces, VLAN interfaces and VRF.

```
admin@SwitchA# set vlans vlan-id 5 l3-interface vlan-5
admin@SwitchA# set vlans vlan-id 6 l3-interface vlan-6
admin@SwitchA# set vlans vlan-id 7 l3-interface vlan-7
admin@SwitchA# set interface gigabit-ethernet te-1/1/30 routed-interface enable true
admin@SwitchA# set interface gigabit-ethernet te-1/1/30 routed-interface name rif-30
admin@SwitchA# set interface gigabit-ethernet te-1/1/23 family ethernet-switching native-vlan-id 6
admin@SwitchA# set interface gigabit-ethernet te-1/1/23 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet te-1/1/23 family ethernet-switching vlan members 5
admin@SwitchA# set interface gigabit-ethernet te-1/1/23 family ethernet-switching vlan members 7
admin@SwitchA# set vlans reserved-vlan 3000-3100
admin@SwitchA# set l3-interface routed-interface rif-30
admin@SwitchA# set ip vrf vrf1
admin@SwitchA# set l3-interface vlan-interface vlan-5 vrf vrf1
admin@SwitchA# set l3-interface vlan-interface vlan-6 vrf vrf1
admin@SwitchA# set l3-interface vlan-interface vlan-6 address 192.168.60.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan-7 vrf vrf1
admin@SwitchA# set l3-interface vlan-interface vlan-7 address 192.168.70.1 prefix-length 24
```

Step 2 Configure EBGP and BGP related configuration.

```
admin@SwitchA# set protocols bgp local-as 65001
```

```
admin@SwitchA# set protocols bgp router-id 49.49.49.49
admin@SwitchA# set protocols bgp interface rif-30 remote-as 65002
admin@SwitchA# set protocols bgp interface rif-30 ipv6-unicast activate true
admin@SwitchA# set protocols bgp interface rif-30 capability extended-nexthop
admin@SwitchA# set protocols bgp ebgp-requires-policy false
admin@SwitchA# set protocols bgp ipv4-unicast network 49.49.49.49/32
admin@SwitchA# set protocols bgp evpn advertise-all-vni
admin@SwitchA# set protocols bgp evpn advertise ipv4-unicast
admin@SwitchA# set protocols bgp evpn advertise ipv6-unicast
admin@SwitchA# set protocols bgp evpn advertise-svi-ip
admin@SwitchA# set protocols bgp vrf vrf1 local-as 65001
admin@SwitchA# set protocols bgp vrf vrf1 router-id 49.49.49.49
admin@SwitchA# set protocols bgp vrf vrf1 ipv4-unicast network 192.168.60.0/24
admin@SwitchA# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@SwitchA# set protocols bgp vrf vrf1 evpn advertise ipv6-unicast
```

Step 3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step 4 Configure VXLAN source interface, VXLAN VNI and map VNI IDs to VLAN IDs. Also create an L3 VNI in vrf1.

```
admin@SwitchA# set vxlans source-interface lo address 49.49.49.49
admin@SwitchA# set vxlans vni 999 vlan 5
admin@SwitchA# set vxlans vni 9991000 vlan 6
admin@SwitchA# set vxlans vni 9991007 vlan 7
admin@SwitchA# set vxlans vrf vrf1 l3-vni 999
```

Step 5 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step 1 Configure physical interfaces, VLAN interfaces and VRF.

```
admin@SwitchB# set vlans vlan-id 5 l3-interface vlan-5
admin@SwitchB# set vlans vlan-id 6 l3-interface vlan-6
admin@SwitchB# set vlans vlan-id 8 l3-interface vlan-8
admin@SwitchB# set interface gigabit-ethernet ge-1/1/30 routed-interface enable true
admin@SwitchB# set interface gigabit-ethernet ge-1/1/30 routed-interface name rif-30
admin@SwitchB# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 6
admin@SwitchB# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching vlan members 5
admin@SwitchB# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching vlan members 8
admin@SwitchB# set vlans reserved-vlan 3000-3100
admin@SwitchB# set l3-interface routed-interface rif-30
admin@SwitchB# set ip vrf vrf1
admin@SwitchB# set l3-interface vlan-interface vlan-5 vrf vrf1
admin@SwitchB# set l3-interface vlan-interface vlan-6 vrf vrf1
admin@SwitchB# set l3-interface vlan-interface vlan-6 address 192.168.60.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan-8 vrf vrf1
admin@SwitchB# set l3-interface vlan-interface vlan-8 address 192.168.80.1 prefix-length 24
```

Step 2 Configure EBGP and BGP related configuration.

```
admin@SwitchB# set protocols bgp local-as 65002
admin@SwitchB# set protocols bgp router-id 57.57.57.57
admin@SwitchB# set protocols bgp interface rif-30 remote-as 65001
admin@SwitchB# set protocols bgp interface rif-30 ipv6-unicast activate true
admin@SwitchB# set protocols bgp interface rif-30 capability extended-nexthop
admin@SwitchB# set protocols bgp ebgp-requires-policy false
admin@SwitchB# set protocols bgp ipv4-unicast network 57.57.57.57/32
admin@SwitchB# set protocols bgp evpn advertise-all-vni
admin@SwitchB# set protocols bgp evpn advertise ipv4-unicast
admin@SwitchB# set protocols bgp evpn advertise ipv6-unicast
admin@SwitchB# set protocols bgp evpn advertise-svi-ip
admin@SwitchB# set protocols bgp vrf vrf1 local-as 65002
```

```
admin@SwitchB# set protocols bgp vrf vrf1 router-id 57.57.57.57
admin@SwitchB# set protocols bgp vrf vrf1 ipv4-unicast network 192.168.80.0/24
admin@SwitchB# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@SwitchB# set protocols bgp vrf vrf1 evpn advertise ipv6-unicast
```

Step 3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step 4 Configure VXLAN source interface, VXLAN VNI and map VNI IDs to VLAN IDs. Also create an L3 VNI in vrf1.

```
admin@SwitchB# set vxlans source-interface lo address 57.57.57.57
admin@SwitchB# set vxlans vni 999 vlan 5
admin@SwitchB# set vxlans vni 9991000 vlan 6
admin@SwitchB# set vxlans vni 9991008 vlan 8
admin@SwitchB# set vxlans vrf vrf1 l3-vni 999
```

Step 5 Commit the configuration.

```
admin@SwitchB# commit
```

Verify the Configuration

- Run the **run l3-interface routed-interface** *<interface-name>* command to check the information of the unnumbered BGP interface.

```
admin@SwitchB# run show l3-interface routed-interface rif-30
rif-30         Hwaddr 18:5A:58:03:35:81, Vlan:3000, MTU: 1500, State:UP
            Inet addr: fe80::1a5a:5810:503:3581/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets................0
```

- Run the **run show bgp neighbor** command to check the BGP neighbor state.

```
admin@SwitchB# run show bgp neighbor
BGP neighbor on rif-30: fe80::1a5a:5820:41f:63a1, remote AS 65001, local AS 65002, external link
Hostname: localhost
  BGP version 4, remote router ID 49.49.49.49, local router ID 57.57.57.57
  BGP state = Established, up for 06:04:23
 ......
```

- Run the **run show bgp evpn route** command to check the EVPN route information.

```
admin@SwitchB# run show bgp evpn route
BGP table version is 6, local router ID is 57.57.57.57
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[IPlen]:[VTEP-IP]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

   Network          Next Hop            Metric LocPrf Weight Path
                    Extended Community
Route Distinguisher: 49.49.49.49:2
*> [5]:[0]:[24]:[192.168.60.0]
                    49.49.49.49              0             0 65001 i
                    RT:65001:999 ET:8 Rmac:18:5a:58:1f:63:a1
Route Distinguisher: 49.49.49.49:3
*> [2]:[0]:[48]:[18:5a:58:1f:63:a1]:[32]:[192.168.60.1]
                    49.49.49.49                           0 65001 i
                    RT:65001:999 RT:65001:9991000 ET:8 Rmac:18:5a:58:1f:63:a1
```

```
*> [2]:[0]:[48]:[18:5a:58:1f:63:a1]:[128]:[fe80::1a5a:5820:21f:63a1]
                    49.49.49.49                             0 65001 i
                    RT:65001:9991000 ET:8
*> [3]:[0]:[32]:[49.49.49.49]
                    49.49.49.49                             0 65001 i
                    RT:65001:9991000 ET:8
Route Distinguisher: 49.49.49.49:4
*> [2]:[0]:[48]:[18:5a:58:1f:63:a1]:[32]:[192.168.70.1]
                    49.49.49.49                             0 65001 i
                    RT:65001:999 RT:65001:9991007 ET:8 Rmac:18:5a:58:1f:63:a1
*> [2]:[0]:[48]:[18:5a:58:1f:63:a1]:[128]:[fe80::1a5a:5820:31f:63a1]
                    49.49.49.49                             0 65001 i
                    RT:65001:9991007 ET:8
*> [3]:[0]:[32]:[49.49.49.49]
                    49.49.49.49                             0 65001 i
                    RT:65001:9991007 ET:8
Route Distinguisher: 57.57.57.57:2
*> [5]:[0]:[24]:[192.168.80.0]
                    57.57.57.57             0         32768 i
                    ET:8 RT:65002:999 Rmac:18:5a:58:03:35:81
Route Distinguisher: 57.57.57.57:3
*> [2]:[0]:[48]:[18:5a:58:03:35:81]:[32]:[192.168.60.2]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991000 RT:65002:999 Rmac:18:5a:58:03:35:81
*> [2]:[0]:[48]:[18:5a:58:03:35:81]:[128]:[fe80::1a5a:5810:203:3581]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991000
*> [3]:[0]:[32]:[57.57.57.57]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991000
Route Distinguisher: 57.57.57.57:4
*> [2]:[0]:[48]:[18:5a:58:03:35:81]:[32]:[192.168.80.1]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991008 RT:65002:999 Rmac:18:5a:58:03:35:81
*> [2]:[0]:[48]:[18:5a:58:03:35:81]:[128]:[fe80::1a5a:5810:403:3581]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991008
*> [3]:[0]:[32]:[57.57.57.57]
                    57.57.57.57                       32768 i
                    ET:8 RT:65002:9991008

Displayed 14 prefixes (14 paths)
```

- Run the **run show vxlan tunnel** command to check the VXLAN tunnel information.

```
admin@SwitchB# run show vxlan tunnel
Total number of tunnels: 2

VNI 999, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:57.57.57.57, dst addr:49.49.49.49, state:UP
  traffic type:unicast
  Vtep type:EVPN
  nexthops:fe80::1a5a:5820:41f:63a1
  output ports:ge-1/1/30

VNI 9991000, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:57.57.57.57, dst addr:49.49.49.49, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:fe80::1a5a:5820:41f:63a1
  output ports:ge-1/1/30
```

- Run the **run show vxlan evpn route** command to check the VXLAN route information.

```
admin@SwitchB# run show vxlan evpn route
VRF       ROUTE             NextHop          VNI         Interface
--------  ----------------  ---------------  ----------  -----------------
vrf1      192.168.60.1/32   49.49.49.49      999         vlan-5
vrf1      192.168.60.0/24   49.49.49.49      999         vlan-5
```

```
vrf1      192.168.70.1/32   49.49.49.49      999         vlan-5
```

- Run the **run show route vrf vrf1** command to check the route information for vrf1.

```
admin@SwitchB# run show route vrf vrf1
show ip route vrf vrf1
======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, A - Babel, F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (blackhole), 06:07:34
B   192.168.60.0/24 [20/0] via 49.49.49.49, vlan-5 onlink, weight 1, 02:03:03
C>* 192.168.60.0/24 is directly connected, vlan-6, 05:38:57
B>* 192.168.60.1/32 [20/0] via 49.49.49.49, vlan-5 onlink, weight 1, 02:03:03
B>* 192.168.70.1/32 [20/0] via 49.49.49.49, vlan-5 onlink, weight 1, 02:03:03
C>* 192.168.80.0/24 is directly connected, vlan-8, 05:38:57


show ipv6 route vrf vrf1
========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       A - Babel, F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

VRF vrf1:
K>* ::/0 [255/8192] unreachable (blackhole), 06:07:36
C * fe80::/64 is directly connected, vlan-8, 05:38:58
C * fe80::/64 is directly connected, vlan-6, 05:38:58
C>* fe80::/64 is directly connected, vlan-5, 06:07:34
```

Configuring BGP Attribute

- Configuring the AS_Path Attribute
- Configuring the BGP Community Attribute
- Configuring the MED Attribute
- Configuring the Next_Hop Attribute

Configuring the AS_Path Attribute

The AS_Path attribute records all the ASs that a route passes through from the source to the destination in the vector order. To prevent inter-AS routing loops, a BGP device does not receive the routes of which the AS_Path list contains the local AS number.

When a BGP speaker advertises an imported route:

- If the route is advertised to EBGP peers, the BGP speaker creates an AS_Path list containing the local AS number in an Update message.
- If the route is advertised to IBGP peers, the BGP speaker creates an empty AS_Path list in an Update message.

When a BGP speaker advertises a route learned in the Update message sent by another BGP speaker:

- If the route is advertised to EBGP peers, the BGP speaker adds the local AS number to the leftmost of the AS_Path list. According to the AS_Path list, the BGP speaker that receives the route can learn about the ASs through which the route passes to reach the destination. The number of the AS that is nearest to the local AS is placed on the top of the AS_Path list. The other AS numbers are listed according to the sequence in which the route passes through ASs.
- If the route is advertised to IBGP peers, the BGP speaker does not change the AS_Path attribute of the route.

You can configure the AS_Path attribute to implement flexible route selection.

Apply a Routing Policy to Routes Advertised

The **set protocols bgp neighbor route-map** command applies a route map to incoming or outgoing routes. It can be used to configure the route map for modifying the AS_Path attribute of the route.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in route-map map1
admin@XorPlus# commit
```

Configure an AS Path List to Advertise or Receive Routes from Peers

The **set protocols bgp neighbor filter-list** command configures an AS Path list to advertise or receive routes from peers.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in filter-list List1
admin@XorPlus# commit
```

Configure BGP to Treat two BGP Routes as Equal Cost ven if AS-paths Differ

he **set protocols bgp bestpath as-path multipath-relax** command configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost even if their AS-paths differ, as long as their AS-path lengths and other relevant attributes are the same. This allows routes with different AS-paths to be programmed into the forwarding table as equal cost multipath routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

```
admin@XorPlus# set protocols bgp bestpath as-path multipath-relax
admin@XorPlus# commit
```

Configuring the BGP Community Attribute

The Community attribute is a private BGP route attribute. It is transmitted between BGP peers and is not restricted within an AS. The Community attribute allows a group of BGP devices in multiple ASs to share the same routing policies, which simplifies routing policy applications and facilitates routing policy management and maintenance. A BGP device can add or change the community attributes of routes to be advertised.

Enable Community Exchange with Peer

The **set protocols bgp neighbor send-community** command enables community and/or extended community exchange with the specified neighbor. When this command is configured for the peer-group, then all the neighbors that are part of peer-group will send the community values to the peers.

The following example allows community values to be sent to a specific neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast send-community both
admin@XorPlus# commit
```

Apply a Routing Policy to Routes Advertised

The **set protocols bgp neighbor route-map** command applies a route map to incoming or outgoing routes. It can be used to configure the route map for modifying the community attribute of the route.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in route-map map1
admin@XorPlus# commit
```

BGP Community Lists

You can use community lists to define a BGP community to tag one or more routes. You can then use the communities to apply a route policy on either egress or ingress.
The BGP community list can be either standard or expanded. The standard BGP community list is a pair of values (such as 100:100) that can be tagged on a specific prefix and advertised to other neighbors or applied on route ingress. Or, it can be one of four BGP default communities:

- **internet**: a BGP community that matches all routes
- **local-AS**: a BGP community that restricts routes to your confederation's sub-AS
- **no-advertise**: a BGP community that is not advertised to anyone
- **no-export**: a BGP community that is not advertised to the eBGP peer

An expanded BGP community list takes a regular expression (BGP Regular Expressions) of communities and matches the listed communities.
When the neighbor receives the prefix, it examines the community value and takes action accordingly, such as permitting or denying the community member in the routing policy.
Here is an example of a standard community list filter:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# commit
```

You can apply the community list to a route map to define the routing policy:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match community COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

Configuring the MED Attribute

The multi-exit discriminator (MED) helps determine the optimal route for incoming traffic of an AS. It is similar to the metric used in IGP. When a BGP device obtains multiple routes to the same destination address but with different next hops from EBGP peers, the BGP device selects the route with the smallest MED value as the optimal route.

- Run the following command to enable comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

  set protocols bgp [***vrf*** <*vrf-name*>] **always-compare-med**

  MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

  During the best-path selection process, MED comparison is done only among paths from the same autonomous system. Use the command bgp always-compare-med to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

- Run the following command to configure a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute.

  set protocols bgp [***vrf*** <*vrf-name*>] **bestpath med missing-as-worst**

Configuring the Next_Hop Attribute

The Next_Hop attribute records the next hop that a route passes through. The Next_Hop attribute of BGP is different from that of an IGP because it may not be the neighbor IP address. A BGP speaker processes the Next_Hop attribute based on the following rules:

- When advertising a route to an EBGP peer, a BGP speaker sets the Next_Hop attribute of the route to the address of the local interface through which the BGP peer relationship is established with the peer.
- When advertising a locally originated route to an IBGP peer, the BGP speaker sets the Next_Hop attribute of the route to the address of the local interface through which the BGP peer relationship is established with the peer.
- When advertising a route learned from an EBGP peer to an IBGP peer, the BGP speaker does not change the Next_Hop attribute of the route.

Configure the Router as the Next Hop for Routes Sent

When an Autonomous System Boundary Router (ASBR) forwards the route learned from an EBGP peer to an IBGP peer, the ASBR does not change the next hop of the route by default. When the IBGP peer receives this route, it finds the next hop unreachable, sets the route to inactive, and does not use this route to guide traffic forwarding. To enable the IBGP peer to use this route to guide traffic forwarding, configure the ASBR to set its IP address as the next hop of the route when the ASBR forwards this route to the IBGP peer. After the IBGP peer receives the route from the ASBR, it finds the next hop of the route reachable, sets the route to active, and uses this route to guide traffic forwarding.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast next-hop-self
admin@XorPlus# commit
```

Apply a Routing Policy to Routes Advertised

The **set protocols bgp neighbor route-map** command applies a route map to incoming or outgoing routes. It can be used to configure the route map for modifying the Next_Hop attribute of the route.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in route-map map1
admin@XorPlus# commit
```

Configuration Examples

- Example for Configuring Basic BGP Functions
- Example for Configuring a BGP Route Reflector
- Example for Configuring BGP Load Balancing

Example for Configuring Basic BGP Functions

- Network Requirement
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
  - Viewing BGP Peer Status on Switch B
  - Configuring Switch A to Advertise Route 192.168.10.0/24
  - Configuring Switch B to Advertise a Connected Route

Network Requirement

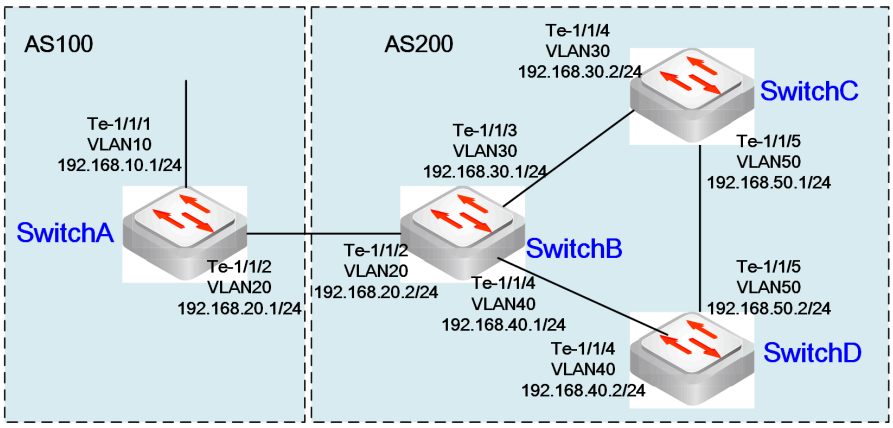
As shown in Figure. 1, BGP runs on all the switches.

An EBGP connection is established between Switch A and Switch B, and IBGP fullmesh connections are established between Switch B, Switch C, and Switch D.

Configure IBGP connections between Switch B, Switch C, and Switch D.

Configure an EBGP connection between Switch A and Switch B.

Figure 1. BGP configuration



Procedure

This section describes the steps of how to configure basic BGP functions on SwitchA, SwitchB, SwitchC and SwitchD.

Switch A

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchA# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchA# set l3-interface vlan-interface vlan10 address 192.168.10.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan20 address 192.168.20.1 prefix-length 24
```

Step2 Configure an EBGP connection.

```
admin@SwitchA# set protocols bgp router-id 1.1.1.1
admin@SwitchA# set protocols bgp local-as 100
admin@SwitchA# set protocols bgp neighbor 192.168.20.2 remote-as 200
admin@SwitchA# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchB# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchB# set vlans vlan-id 40 l3-interface vlan40
admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchB# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 30
admin@SwitchB# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 40
admin@SwitchB# set l3-interface vlan-interface vlan20 address 192.168.20.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan30 address 192.168.30.1 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan40 address 192.168.40.1 prefix-length 24
```

Step2 Configure EBGP and IBGP connections.

```
admin@SwitchB# set protocols bgp router-id 2.2.2.2
admin@SwitchB# set protocols bgp local-as 200
admin@SwitchB# set protocols bgp neighbor 192.168.20.1 remote-as 100
admin@SwitchB# set protocols bgp neighbor 192.168.30.2 remote-as 200
admin@SwitchB# set protocols bgp neighbor 192.168.40.2 remote-as 200
admin@SwitchB# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchC# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchC# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchC# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 30
admin@SwitchC# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 50
admin@SwitchC# set l3-interface vlan-interface vlan30 address 192.168.30.2 prefix-length 24
admin@SwitchC# set l3-interface vlan-interface vlan50 address 192.168.50.1 prefix-length 24
```

Step2 Configure the IBGP connection.

```
admin@SwitchC# set protocols bgp router-id 3.3.3.3
admin@SwitchC# set protocols bgp local-as 200
admin@SwitchC# set protocols bgp neighbor 192.168.30.1 remote-as 200
admin@SwitchC# set protocols bgp neighbor 192.168.50.2 remote-as 200
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Switch D

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchD# set vlans vlan-id 40 l3-interface vlan40
```

```
admin@SwitchD# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchD# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 40
admin@SwitchD# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 50
admin@SwitchD# set l3-interface vlan-interface vlan40 address 192.168.40.2 prefix-length 24
admin@SwitchD# set l3-interface vlan-interface vlan50 address 192.168.50.2 prefix-length 24
```

Step2 Configure the IBGP connection.

```
admin@SwitchD# set protocols bgp router-id 4.4.4.4
admin@SwitchD# set protocols bgp local-as 200
admin@SwitchD# set protocols bgp neighbor 192.168.40.1 remote-as 200
admin@SwitchD# set protocols bgp neighbor 192.168.50.1 remote-as 200
```

Step3 Enable IP routing.

```
admin@SwitchD# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchD# commit
```

Viewing BGP Peer Status on Switch B

```
admin@SwitchB# run show bgp neighbor
BGP neighbor on vlan20: 192.168.20.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 1.1.1.1, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  Waiting for Peer IPv6 LLA
BGP Connect Retry Timer in Seconds: 120
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.30.2, remote AS 200, local AS 200, internal link
 Administratively shut down
  BGP version 4, remote router ID 3.3.3.3, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
```

```
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 600 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.40.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 4.4.4.4, local router ID 2.2.2.2
  BGP state = Active
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1
```

Configuring Switch A to Advertise Route 192.168.10.0/24

```
admin@SwitchA# set protocols bgp ipv4-unicast network 192.168.10.0/24
admin@SwitchA# commit
```

View the BGP routing table of Switch B:

```
admin@SwitchB# run show bgp
show bgp ipv4 unicast
=====================
BGP table version is 2, local router ID is 4.4.4.4, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0/24
                    192.168.20.1             0             100 32768 i

Displayed  1 routes and 1 total paths


show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

View the BGP routing table of Switch C:

```
admin@SwitchC# run show bgp
show bgp ipv4 unicast
=====================
BGP table version is 2, local router ID is 3.3.3.3, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0/24
                    192.168.20.1             0             100 32768 i

Displayed  1 routes and 1 total paths


show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

The preceding command output display that the route to destination 192.168.10.0/24 becomes invalid because the next hop address of this route is unreachable.

Configuring Switch B to Advertise a Connected Route

```
admin@SwitchB# set protocols bgp ipv4-unicast redistribute connected
admin@SwitchB# commit
```

Ping 192.168.10.1 on Switch C:

```
admin@SwitchC# run ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_req=1 ttl=63 time=4.68 ms
64 bytes from 192.168.10.1: icmp_req=2 ttl=63 time=4.46 ms
64 bytes from 192.168.10.1: icmp_req=3 ttl=63 time=5.35 ms
```

```
64 bytes from 192.168.10.1: icmp_req=4 ttl=63 time=4.52 ms
64 bytes from 192.168.10.1: icmp_req=5 ttl=63 time=4.51 ms
192.168.10.1 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 4.460/4.709/5.358/0.338 ms
```

View the BGP routing table of Switch C:

```
admin@SwitchC# run show bgp
show bgp ipv4 unicast
=====================
BGP table version is 2, local router ID is 3.3.3.3, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0/24
                    192.168.20.1             0             100 32768 i
*> 192.168.40.0/24
                    192.168.30.1             0             100 32768 i
   192.168.30.0/24
                    192.168.30.1             0             100 32768 i
*> 192.168.10.0/24
                    192.168.30.1             0             100 32768 i

Displayed  4 routes and 4 total paths


show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

Example for Configuring a BGP Route Reflector

- Network Requirement
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
  - Configuring Switch A to Advertise Route 192.168.10.0/24
- Verify the Configurations

Network Requirement

As shown in **Figure. 1**, BGP runs on all the switches.

An EBGP connection is established between Switch A and Switch B, and IBGP fullmesh connections are established between Switch B, Switch C, and Switch D.

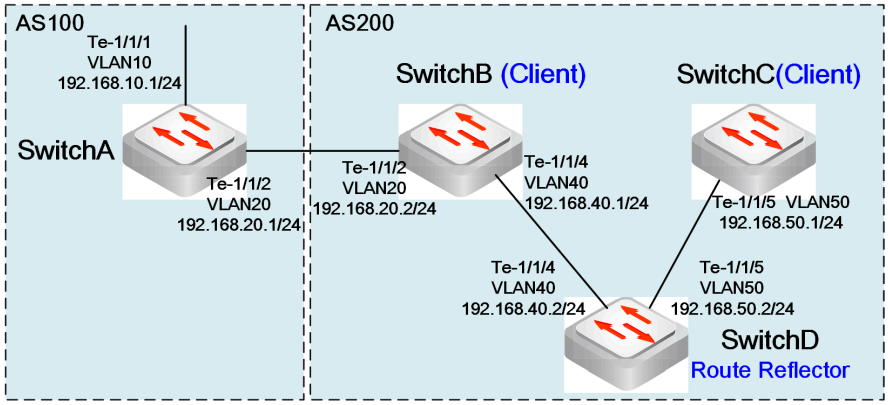
Configure IBGP connections between Switch B, Switch C, and Switch D.

Configure an EBGP connection between Switch A and Switch B.

Configure Switch D as the route reflector for Switch B and Switch C, which is the clients of Switch D, to simplify device configuration and management.

You have to finish configurations on Switch D to be a route reflector. No configuration is required on the client.

Figure 1. BGP Route Reflector Configuration



Procedure

This section describes the steps to configure basic BGP functions on SwitchA, SwitchB, SwitchC and SwitchD, configure Switch D as the route reflector for Switch B and Switch C.

Switch A

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchA# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchA# set l3-interface vlan-interface vlan10 address 192.168.10.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan20 address 192.168.20.1 prefix-length 24
```

Step2 Configure an EBGP connection.

```
admin@SwitchA# set protocols bgp router-id 1.1.1.1
admin@SwitchA# set protocols bgp local-as 100
admin@SwitchA# set protocols bgp neighbor 192.168.20.2 remote-as 200
admin@SwitchA# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchB# set vlans vlan-id 40 l3-interface vlan40
admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchB# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 40
admin@SwitchB# set l3-interface vlan-interface vlan20 address 192.168.20.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan40 address 192.168.40.1 prefix-length 24
```

Step2 Configure EBGP and IBGP connections.

```
admin@SwitchB# set protocols bgp router-id 2.2.2.2
admin@SwitchB# set protocols bgp local-as 200
admin@SwitchB# set protocols bgp neighbor 192.168.20.1 remote-as 100
admin@SwitchB# set protocols bgp neighbor 192.168.40.2 remote-as 200
admin@SwitchB# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchC# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchC# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 50
admin@SwitchC# set l3-interface vlan-interface vlan50 address 192.168.50.1 prefix-length 24
```

Step2 Configure the IBGP connection.

```
admin@SwitchC# set protocols bgp router-id 3.3.3.3
admin@SwitchC# set protocols bgp local-as 200
admin@SwitchC# set protocols bgp neighbor 192.168.50.2 remote-as 200
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Switch D

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchD# set vlans vlan-id 40 l3-interface vlan40
admin@SwitchD# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchD# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 40
admin@SwitchD# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 50
admin@SwitchD# set l3-interface vlan-interface vlan40 address 192.168.40.2 prefix-length 24
admin@SwitchD# set l3-interface vlan-interface vlan50 address 192.168.50.2 prefix-length 24
```

Step2 Configure the IBGP connection.

```
admin@SwitchD# set protocols bgp router-id 4.4.4.4
admin@SwitchD# set protocols bgp local-as 200
admin@SwitchD# set protocols bgp neighbor 192.168.40.1 remote-as 200
admin@SwitchD# set protocols bgp neighbor 192.168.50.1 remote-as 200
```

Step3 Configure Switch D to be a route reflector for Switch B and Switch C.

```
admin@SwitchD# set protocols bgp neighbor 192.168.40.1 ipv4-unicast route-reflector-client
admin@SwitchD# set protocols bgp neighbor 192.168.50.1 ipv4-unicast route-reflector-client
```

Step4 Enable IP routing.

```
admin@SwitchD# set ip routing enable true
```

Step5 Commit the configurations.

```
admin@SwitchD# commit
```

Configuring Switch A to Advertise Route 192.168.10.0/24

```
admin@SwitchA# set protocols bgp ipv4-unicast network 192.168.10.0/24
admin@SwitchA# commit
```

Verify the Configurations

- View the BGP routing table of Switch D.

```
admin@SwitchD# run show bgp route 192.168.10.0/24
BGP routing table entry for 192.168.10.0/24
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  192.168.50.2
  200
    192.168.10.0 from 192.168.20.1 (2.2.2.2)
      Origin IGP, metric 0, valid, external, best (First path received)
      Last update: Wed Apr  7 16:13:35 2021
```

Example for Configuring BGP Load Balancing

- Network Requirement
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
  - Viewing BGP Peer Status on Switch B
  - Configuring Switch D to Advertise Route 192.168.10.0/24
  - Configure Switch A to Enable BGP Load Balancing

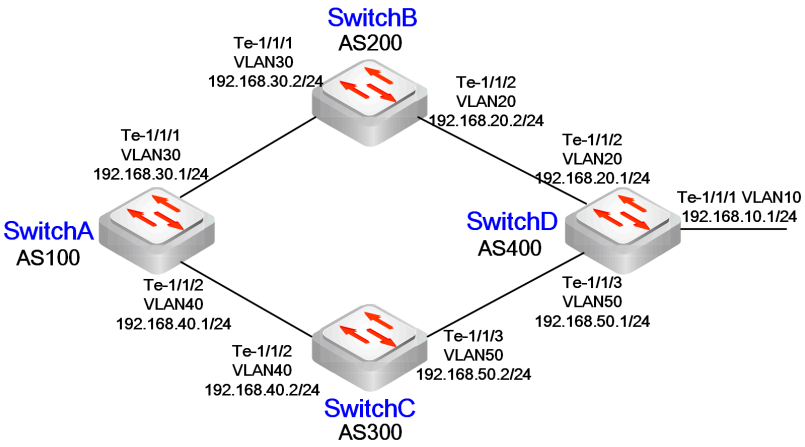
Network Requirement

Configure load balancing on Switch A.

Configure EBGP connections between Switch B and Switch A and between Switch B and Switch D.

Configure EBGP connections between Switch C and Switch A and between Switch C and Switch D.

Figure 1. BGP Load Balancing



Procedure

Switch A

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchA# set vlans vlan-id 40 l3-interface vlan40
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 30
admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 40
admin@SwitchA# set l3-interface vlan-interface vlan30 address 192.168.30.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan40 address 192.168.40.1 prefix-length 24
```

Step2 Configure an EBGP connection.

```
admin@SwitchA# set protocols bgp router-id 1.1.1.1
admin@SwitchA# set protocols bgp local-as 100
admin@SwitchA# set protocols bgp neighbor 192.168.30.2 remote-as 200
admin@SwitchA# set protocols bgp neighbor 192.168.40.2 remote-as 300
admin@SwitchA# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchB# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 30
admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchB# set l3-interface vlan-interface vlan20 address 192.168.20.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan30 address 192.168.30.2 prefix-length 24
```

Step2 Configure EBGP connections.

```
admin@SwitchB# set protocols bgp router-id 2.2.2.2
admin@SwitchB# set protocols bgp local-as 200
admin@SwitchB# set protocols bgp neighbor 192.168.30.1 remote-as 100
admin@SwitchB# set protocols bgp neighbor 192.168.20.1 remote-as 400
admin@SwitchB# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchC# set vlans vlan-id 40 l3-interface vlan40
admin@SwitchC# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchC# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 40
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 50
admin@SwitchC# set l3-interface vlan-interface vlan40 address 192.168.40.2 prefix-length 24
admin@SwitchC# set l3-interface vlan-interface vlan50 address 192.168.50.2 prefix-length 24
```

Step2 Configure the EBGP connection.

```
admin@SwitchC# set protocols bgp router-id 3.3.3.3
admin@SwitchC# set protocols bgp local-as 300
admin@SwitchC# set protocols bgp neighbor 192.168.40.1 remote-as 100
admin@SwitchC# set protocols bgp neighbor 192.168.50.1 remote-as 400
admin@SwitchC# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Switch D

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchD# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchD# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchD# set vlans vlan-id 50 l3-interface vlan50
admin@SwitchD# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
```

```
admin@SwitchD# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@SwitchD# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 50
admin@SwitchD# set l3-interface vlan-interface vlan10 address 192.168.10.1 prefix-length 24
admin@SwitchD# set l3-interface vlan-interface vlan20 address 192.168.20.1 prefix-length 24
admin@SwitchD# set l3-interface vlan-interface vlan50 address 192.168.50.1 prefix-length 24
```

Step2 Configure the EBGP connection.

```
admin@SwitchD# set protocols bgp router-id 4.4.4.4
admin@SwitchD# set protocols bgp local-as 400
admin@SwitchD# set protocols bgp neighbor 192.168.20.2 remote-as 200
admin@SwitchD# set protocols bgp neighbor 192.168.50.2 remote-as 300
admin@SwitchD# set protocols bgp ebgp-requires-policy false
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@SwitchD# commit
```

Viewing BGP Peer Status on Switch B

```
admin@SwitchB# run show bgp neighbor
BGP neighbor on vlan30: 192.168.30.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 1.1.1.1, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  Waiting for Peer IPv6 LLA
BGP Connect Retry Timer in Seconds: 120
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.20.2, remote AS 400, local AS 200, internal link
 Administratively shut down
  BGP version 4, remote router ID 3.3.3.3, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
```

```
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 600 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.40.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 4.4.4.4, local router ID 2.2.2.2
  BGP state = Active
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
```

```
Read thread: off  Write thread: off  FD used: -1
```

Configuring Switch D to Advertise Route 192.168.10.0/24

```
admin@SwitchD# set protocols bgp ipv4-unicast network 192.168.10.0/24
admin@SwitchD# commit
```

Configure Switch A to Enable BGP **Load Balancing**

Because Switch A has two routes to reach AS 400, configuring load balancing over the two BGP routes on Switch A can improve link usage.

```
admin@SwitchA# set protocols bgp ipv4-unicast multipath ebgp maximum-paths 2
admin@SwitchA# commit
```

Then you can view the BGP routing table to 192.168.10.0/24 on Switch A, you can find that:

- The route 192.168.10.0/24 has two next hops, 192.168.30.2 and 192.168.40.2, both of which are marked with a greater-than sign (>), indicating that they are the optimal routes.
- By using the **run show bgp route 192.168.10.0/24** command, you can find two routes to 192.168.10.0/24. One has next hop 192.168.30.2 and output interface VLAN interface vlan30, and the other has next hop 192.168.40.2 and output interface VLAN interface vlan40.

Routing Map Configuration

This section describes how to use routing map to filter routes and change route attributes.

- Routing Map Introduction
- Configuring Filters
  - Configuring a Community Filter
  - Configuring a Large Community Filter
  - Configuring an AS_Path Filter
  - Configuring an Extended Community Filter
  - Configuring an IP Prefix List
- Configuring a Routing Map
- Example for Filtering the Routes to Be Advertised and Receiving

Routing Map Introduction

A routing policy uses different matching rules and modes to select routes and change route attributes. There are different filters in the routing policy that can be used independently to filter routes in specific scenarios.

Matching Rule

A routing map is a routing policy consists of *N* nodes of match and set statements (*N* ≥ 1). Each node has its own set of **match** clauses that must be matched in order to accept a policy. The **match** clauses define matching rules related to route attributes and filters. The system checks routes in the orders of a routing map in ascending order of order IDs.

When a route matches all **match** clauses in a order, the route enters the matching modes defined in **matching-policy** and **set-action** clauses and stops checking **match** clauses in other nodes. The two supported matching modes are:

- **permit**: A route is permitted, and actions defined by **set-action** clauses are performed on the route to set its attributes.
- **deny**: A route is denied.

If a route does not match any **match** clause in a node, the route is passed to the next node. If the route does not match any node, the route is filtered out.

Note that, in all configurations, **matching-policy** is a required clause to enable a route map. Other clauses are optional.

The default action of a route-map, if no entries match, is to deny. I.e. a route-map essentially has as its last entry an empty deny entry, which matches all routes. To change this behaviour, one must specify an empty permit entry as the last entry in the route-map.

Filters

There are different filters specified in **match** clauses in a routing policy which including IP prefix list, AS_Path filter, community filter, extended community filter, and large community filter. These filters have their own matching rules and modes and can be used independently to filter routes in specific situations. The following offers a brief explanation to each of these filters.

IP Prefix List

IP prefix lists filter routes based on the IP prefixes of the source IP address, destination IP address, and next-hop IP address of packets. They can be used independently when routing protocols advertise and receive routes.

Each IP prefix list consists of multiple indexes, and each index matches a node. An IP prefix list checks routes in the nodes of a routing policy in ascending order of sequence numbers. If a route matches one node, the route is not checked by additional nodes. If a route does not match any one of the nodes, the route is filtered out.

The IP prefix list supports exact matching or matching within a specified mask length.

> **NOTE:**
> - When an IP address is 0.0.0.0 (a wildcard address), all routes in the mask length range are permitted or denied.
> - When configuring IP prefix list, it is strongly recommended to configure sequence number for each IP prefix list node. Otherwise, the precedence of this IP prefix list will be uncertain, and thus the desired IP filtering effect will not be achieved.

AS_Path Filter

The AS_Path filter uses the AS_Path attribute of BGP to filter routes. It can be used independently when BGP advertises and receives routes.

The AS_Path attribute records all ASs that a route passes through. For details about the AS_Path attribute, see Configuring the AS_Path Attribute.

Community Filter

The community filter uses the community attribute of BGP to filter routes. It can be used independently when BGP advertises and receives routes.

The community attribute identifies a group of routes with the same properties. For details about the community attribute, see Configuring the BGP Community Attribute.

Extended Community Filter

The extended community filter uses the extended community attribute of BGP to filter routes. It can be used independently when VPN targets are used to identify routes in a VPN.

Large Community Filter

The large community filter uses the large community attribute of BGP to filter routes. The commands **set routing large-community-list {standard <***large-community-list-name***>| seq-standard***<integer>***} {deny|permit}** [**large-community** *<large-community-number>*] and **set routing large-community-list {expanded** *<large-community-list-name>*| **seq-expanded** *<integer>*} **{deny|permit} regex** *<line>* can be used to define the large community list.

Configuring Filters

- Configuring a Community Filter
- Configuring a Large Community Filter
- Configuring an AS_Path Filter
- Configuring an Extended Community Filter
- Configuring an IP Prefix List

Configuring a Community Filter

The community attribute identifies routes with the same characteristics without considering IP prefixes and AS numbers. Configuring community filters and community attributes simplifies route management when it is inconvenient to use the IP prefix list or AS_Path filter. For example, a company branch needs to receive routes only from its headquarters and from branches in adjacent countries. In this case, you can configure different community attributes for each of the branches. Routes in the original branch can then be managed based on community attributes, without considering IP prefixes and AS numbers of routes in different countries.

Community filters are classified into standard and expanded community filters. An expanded community filter supports regular expressions (BGP Regular Expressions) and is more flexible than a standard community filter.

- To configure a standard community filter, run the following command:

set routing community-list standard <*community-list-name*> **{deny|permit} [local-as|no-advertise|no-export|internet|community** <*community*>**]**

- To configure an expanded community filter, run the following command:

set routing community-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

The following example configures a standard community list filter:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# commit
```

Configuring a Large Community Filter

The BGP Large Communities attribute was introduced in Feb 2017 with RFC 8092.
The BGP Large Communities Attribute is similar to the BGP Communities Attribute except that it has 3 components instead of two and each of which are 4 octets in length. Large Communities bring additional functionality and convenience over traditional communities, specifically the fact that the GLOBAL part below is now 4 octets wide allowing seamless use in networks using 4-byte ASNs.
GLOBAL:LOCAL1:LOCAL2 This is the format to define Large Community values.

- To configure a standard large community filter, run the following command:

set routing large-community-list {standard <*large-community-list-name***>| seq-standard**<*integer*>} **{deny|permit}** [**large-community** <*large-community-number*>]

- To configure an expanded large community filter, run the following command:

set routing large-community-list {expanded <*large-community-list-name*>| **seq-expanded** <*integer*>} **{deny|permit} regex** <*line*>

The following example configures a standard large community filter:

```
admin@Xorplus# set routing large-community-list standard LargeCom deny large-community 6215:22:33
admin@Xorplus# commit
```

Configuring an AS_Path Filter

An AS_Path filter is used to filter routes based on the AS_Path attributes of BGP routes. If you do not want to receive routes of a specified AS number, configure an AS_Path filter based on the specified AS number. On a complex network, multiple ACLs or IP prefix lists must be configured to filter BGP routes. This can be a complicated process; configuring an AS_Path filter can simplify the configuration.

You can use the following command to configure the AS_Path filter.

set routing as-path-list <*as-path-list-name*> **{deny|permit} regex** <*txt*>

The following example configures an AS Path list, permit routes that contain 20 in the AS_Path to pass through.

```
admin@Xorplus# set routing as-path-list Aslist permit regex _20_
admin@Xorplus# commit
```

Configuring an Extended Community Filter

You can use an extended community filter when using the route target (RT) attribute to filter routes.

- To configure a standard extended community filter, run the following command:

set routing extcommunity-list standard <*community-list-name*> **{deny|permit} {rt|soo} extcommunity** <*extcommunity*>

- To configure an expanded extended community filter, run the following command:

set routing extcommunity-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

The following example configures a standard extended community filter:

```
admin@Xorplus# set routing extcommunity-list standard EXTcom1 permit rt extcommunity 20
admin@Xorplus# commit
```

Configuring an IP Prefix List

Configuring an IP prefix list controls the advertising and receiving of routes based on the destination address.

You can use the following command to configure the IPv4 prefix list.

set routing prefix-list {ipv4-family <*ipv4-prefix-name*> | **ipv6-family** <*ipv6-prefix-name*>} [**seq** <*sequence-number*>] {**deny|permit} {prefix** <*ipv4/prefixlen*> **[ge <***greater-equal-value***>] [le <***less-equal-value***>]** | **prefix-any**}

> **NOTE:**
> - If an IP prefix list is not used together with the **match** clauses in a routing map, you must set at least one node to the **permit** mode in the IP prefix list. If no node is set to the **permit** mode, all routes are filtered out.
> - When configuring IP prefix list, it is strongly recommended to configure sequence number for each IP prefix list node. Otherwise, the precedence of this IP prefix list will be uncertain, and thus the desired IP filtering effect will not be achieved.

The following example configures the IP prefix list named **p1** to permit only the routes with the mask length ranging from 8 to 16 on the network segment 35.0.0.0/8.

```
admin@Xorplus# set routing prefix-list ipv4-family p1 seq 1 permit prefix 35.0.0.0/8 ge 16
admin@Xorplus# commit
```

Configuring a Routing Map

- Creating a matching-policy Clause
- (Optional) Configuring a match Clause
- (Optional) Configuring a set-action Clause
- Checking the Configuration

A routing map can consist of multiple matching policies, multiple match rules and set-action actions.

Creating a matching-policy Clause

> **NOTE:**
> You should set at least one node to the **permit** mode in a routing policy; otherwise, all routes are filtered out.

The following example create a route map matching policy.

```
admin@Xorplus# set routing route-map GlobalMap order 1 matching-policy permit
admin@Xorplus# commit
```

(Optional) Configuring a match Clause

A **match** clause defines matching rules related to route filters and attributes in a routing policy.

If no **match** clause is configured for a node in a routing policy, routes match the routing policy in this node. If one or more **match** clauses are configured in a node, the relationship between the clauses is "AND". This means that a route matches this node only when they match all the **match** clauses in this node.

> **NOTE:**
> If a **match** clause defines a filter that is not configured, all routes match this **match** clause by default.

The command **set routing route-map <***route-map-name***> order <***NUMBER***> match xx** can be used for configure routing map match clause. PICOS supports most of the route filter parameters, for details about each match clause, see Route Map Commands.

The following commands configure a match clause in the route map to match the community list:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

(Optional) Configuring a set-action Clause

A **set-action** clause specifies the action of setting attributes for routes that have matched a routing policy node. If a node does not have a **set-action** clause configured, the node will only filter routes. If one or more **set-action** clauses are configured in a node, all the **set-action** clauses are applied to routes that have matched the node.

The command **set routing route-map <***route-map-name***> order <***NUMBER***> set-action xx** can be used for configure routing map **set-action** clause. PICOS supports to set most of the several route parameters, for details about each set-action clause, see Route Map Commands.

The following commands configure a match clause in the route map to match the community list and change the community value to 11:101:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# set routing route-map GlobalMap order 10 set-action community 11:101
admin@Xorplus# commit
```

Checking the Configuration

Run the **run show routing route-map** command to check information about the route-policy.

```
admin@Xorplus# run show routing route-map
ZEBRA:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
```

```
  Action:
    Exit routemap
OSPF:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
    community COMMUNITY1
  Set clauses:
    community 11:101
  Call clause:
  Action:
    Exit routemap
```

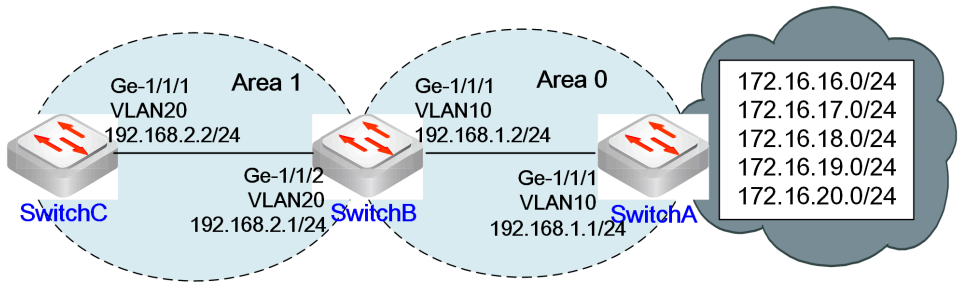
Example for Filtering the Routes to Be Advertised and Receiving

- Network Requirement
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Configure Static Routes on SwitchA
  - Configure a Policy for Advertising Routes on SwitchA
  - Configure a Policy for Receiving Routes on SwitchB

Network Requirement

Figure 1 shows on an OSPF network, how SwitchA receives routes from the Internet and provides these routes for the OSPF network. By configuring the routing map, users on the OSPF network are only allowed to access only the network segments 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24, and do not allow Area 1 to access the IP 1.1.1.1/32 of the loopback address of SwitchA.

Figure 1. Networking diagram for filtering the advertised routes



To implement the route filtering function as above, follow the configuration described below:

1. Configure a routing policy on SwitchA and apply the routing policy during route advertisement. When routes are advertised, the routing policy allows SwitchA to provide routes from network segments 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24 for SwitchB, and allows devices on the OSPF network to access the three network segments.
2. To implement that not allow Area 1 to access the IP 1.1.1.1/32 of the loopback address of SwitchA. Configure a prefix list of "**deny 1.1.1.1/32**" and a "**prefix-any**", and apply to OSPF filter in policy on SwitchB.

Procedure

Switch A

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchA# set vlans vlan-id 10 l3-interface 10
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchA# set l3-interface vlan-interface 10 address 192.168.1.1 prefix-length 24
admin@SwitchA# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
```

Step2 Configure basic OSPF functions.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf area 0
admin@SwitchA# set protocols ospf network 192.168.1.0/24 area 0
admin@SwitchA# set protocols ospf network 1.1.1.1/32 area 0
```

Step3 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchB# set vlans vlan-id 10 l3-interface 10
admin@SwitchB# set vlans vlan-id 20 l3-interface 20
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
```

```
admin@SwitchB# set l3-interface vlan-interface 10 address 192.168.1.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface 20 address 192.168.2.1 prefix-length 24
```

Step2 Configure basic OSPF functions.

```
admin@SwitchB# set protocols ospf router-id 2.2.2.2
admin@SwitchB# set protocols ospf area 0
admin@SwitchB# set protocols ospf area 1
admin@SwitchB# set protocols ospf network 192.168.1.0/24 area 0
admin@SwitchB# set protocols ospf network 192.168.2.0/24 area 1
```

Step3 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure the VLANs and VLAN interfaces.

```
admin@SwitchC# set vlans vlan-id 20 l3-interface 20
admin@SwitchC# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@SwitchC# set l3-interface vlan-interface 20 address 192.168.2.1 prefix-length 24
```

Step2 Configure basic OSPF functions.

```
admin@SwitchC# set protocols ospf router-id 3.3.3.3
admin@SwitchC# set protocols ospf area 1
admin@SwitchC# set protocols ospf network 192.168.2.0/24 area 1
```

Step3 Commit the configurations.

```
admin@SwitchC# commit
```

Configure Static Routes on SwitchA

Configure five static routes on SwitchA and import these routes into OSPF.

```
admin@SwitchA# set protocols static route 172.16.16.0/24 null0
admin@SwitchA# set protocols static route 172.16.17.0/24 null0
admin@SwitchA# set protocols static route 172.16.18.0/24 null0
admin@SwitchA# set protocols static route 172.16.19.0/24 null0
admin@SwitchA# set protocols static route 172.16.20.0/24 null0
admin@SwitchA# set protocols ospf redistribute static
admin@SwitchA# commit
```

Check the IP routing table on SwitchB. You can see that the five static routes are imported into OSPF.

```
admin@SwitchA# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 172.16.16.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.17.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.18.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.19.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.20.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O   192.168.1.0/24 [110/10] is directly connected, 10, weight 1, 00:36:27
O   192.168.2.0/24 [110/10] is directly connected, 20, weight 1, 00:34:56
```

Configure a Policy for Advertising Routes on SwitchA

Configure an IP prefix list named **a2b** on SwitchA.

```
admin@SwitchA# set routing prefix-list ipv4-family a2b seq 10 permit prefix 172.16.17.0/24
admin@SwitchA# set routing prefix-list ipv4-family a2b seq 20 permit prefix 172.16.18.0/24
admin@SwitchA# set routing prefix-list ipv4-family a2b seq 30 permit prefix 172.16.19.0/24
```

Configure a policy for advertising routes on SwitchA, and use the IP prefix list **a2b** to filter routes.

```
admin@SwitchA# set routing route-map a2b order 1 match ipv4-addr address prefix-list a2b
admin@SwitchA# set routing route-map a2b order 1 matching-policy permit
admin@SwitchA# commit
```

Add route-map **a2b** when redistribute static route to OSPF route table.

```
admin@SwitchA# set protocols ospf redistribute static route-map a2b
admin@SwitchA# commit
```

Check the IP routing table on SwitchB. You can see that SwitchB receives only three routes defined in **a2b**.

```
admin@SwitchB# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 172.16.17.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.18.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O>* 172.16.19.0/24 [110/20] via 192.168.1.1, 10, weight 1, 00:02:01
O   192.168.1.0/24 [110/10] is directly connected, 10, weight 1, 00:36:27
O   192.168.2.0/24 [110/10] is directly connected, 20, weight 1, 00:34:56
```

Configure a Policy for Receiving Routes on SwitchB

Configure an IP prefix list named **filter_in** on SwitchB to deny route with prefix 1.1.1.1/32. Note that as there is a "**deny all**" command implicitly configured at the end of all prefix list, do not forget to configure a "**permit prefix-any**" command to allow other routes.

```
admin@SwitchB# set routing prefix-list ipv4-family filter_in seq 10 deny prefix 1.1.1.1/32
admin@SwitchB# set routing prefix-list ipv4-family filter_in seq 20 permit prefix-any
```

Configure a OSPF filter policy for receiving routes on SwitchB, and use the IP prefix list **filter_in** to filter routes.

```
admin@SwitchB# set protocols ospf area 1 in filter-list prefix filter_in
admin@SwitchB# commit
```

Check the IP routing table on SwitchC. You can see that SwitchC does not receive the route 1.1.1.1/32.

```
admin@SwitchC# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 172.16.17.0/24 [110/20] via 192.168.2.1, 20, weight 1, 00:27:16
O>* 172.16.18.0/24 [110/20] via 192.168.2.1, 20, weight 1, 00:27:16
O>* 172.16.19.0/24 [110/20] via 192.168.2.1, 20, weight 1, 00:27:16
O>* 192.168.1.0/24 [110/20] via 192.168.2.1, 20, weight 1, 00:27:17
O   192.168.2.0/24 [110/10] is directly connected, 20, weight 1, 00:28:32
```

IPv6 Support

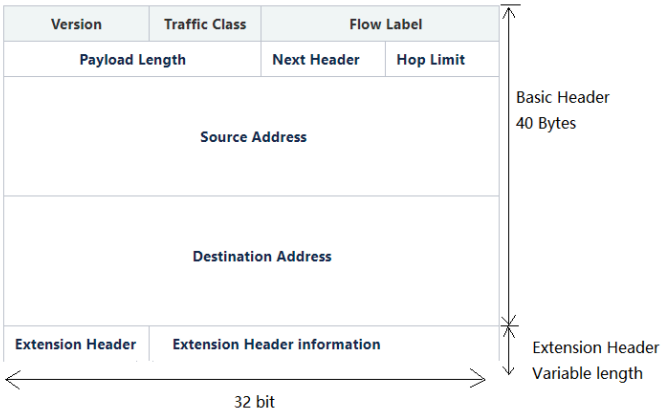
Please note that the N22XX series switches do not support IPv6.

IPv6 Basics

Due to an increased demand for IP addresses across the globe with the introduction of technologies like Internet of Things (IOT), the number of available IP addresses in the IPv4 pool is quickly running out. IPv6 was developed as a replacement for IPv4. An IPv4 address is a 32 bit number where as IPv6 is 128 bits in length and hence has far larger capacity to generate enough IPv6 addresses to cater to the needs of modern IP based networking. In this section we'll discuss some basics of IPv6 addressing including its packet format.

IPv6 Header Format

The IPv6 header format is shown in Figure 1 below.



IPv6 Packet Header

Version is a 4-bit IP protocol version number and is equal to 6.

Traffic Class is an 8-bit field which specifies the traffic class of the IPv6 packet. It is an equivalent of TOS field in IPv4 packet and used in QoS.

Flow Label is 20-bit long and used to differentiate IPv6 traffic. A data flow cab be identified with a source IP and flow label. This field is used by intermediate network devices to differentiate flows.

Payload Length is a 16-bit long field that specifies the length of IPv6 payload following the header including any extension headers in bytes.

Next Header is an 8-bit field and identifies the type of the first extension header that follows the IPv6 basic header or the protocol type of the upper layer PDU.

Hop Limit is 8-bit long and specifies the number of hops the packets can pass. This value is decremented each time the packet passes through a hop and is discarded when the value becomes zero.

Source Address is 128-bit long and defines the source IPv6 address.

Destination Address is also 128-bit long and specifies the destination IPv6 address.

IPv6 uses extension headers between the IPv6 basic header and the upper layer PDU to enhance flexibility in processing IPv6 packets. These extension headers are similar to the Options field in IPv4 packets but unlike IPv4 Options, the header extensions are of variable length to facilitate packet processing. For more information on IPv6 extension headers click here to see IPv6 RFC.

Since version 4.1.0, PICOS fully supports IPv6.

IPv6 Neighbor Discovery Protocol

Neighbor Discovery Protocol (NDP) is part of the Internet Protocol Suite and is used for gathering various network related information. It operates at the link layer in the IP model of layered communication. NDP defines five ICMPv6 packet types for **Router Solicitation**, **Router Advertisement**, **Neighbor Solicitation**, **Neighbor Advertisement** and **Redirect**. NDP is similar in functionality to Address Resolution Protocol (ARP) but the major difference is that ARP is designed to work with IPv4 whereas NDP is designed for IPv6. These ICMPv6 packet types are further explained below.

1. **Router Solicitation--Type-133 (RS):** Router solicitation messages are used by IPv6 capable devices to try to acquire routers on the link. Routers on the link receiving these messages immediately reply with **Router Advertisement** messages. Normally routers periodically advertise themselves on the link but in the case of receiving an RS message the routers respond immediately with Router Advertisement message.
2. **Router Advertisement--Type-134 (RA):** Router advertisements are issued by routers on the link to periodically advertise their presence or these messages can be issued in response to a RS message.
3. **Neighbor Solicitation--Type-135 (NS):** Neighbor solicitation messages are issued by devices on the link to acquire the link layer address of a device or to verify that a neighbor is still alive on the link via cached link layer address.
4. **Neighbor Advertisement--Type-136 (NA):** Neighbor advertisement messages are issued in response to Neighbor Solicitation messages.
5. **Redirect--Type-137:** These messages are used by routers to inform hosts of a better first host router for a destination.

These messages provide the combined functionality listed below.

- **Router Discovery**
- **Prefix Discovery**
- **Parameter Discovery**
- **Address Autoconfiguration**
- **Address Resolution**
- **Next Hop Determination**
- **Neighbor Unreachability Detection**
- **Duplicate Address Detection**
- **DNS and Recursive DNS Search List Via RA Options**
- **Packet Redirection for better next hop**

- IPv6 Neighbor Discovery Configuration
- PICOS L2/L3 Support for IPv6
- Enable Path MTU Discovery

IPv6 Neighbor Discovery Configuration

In this section we will demonstrate briefly the commands used to configure some of the most common IPv6 Neighbor Discovery (ND) features. All these commands apply to layer 3 VLAN interfaces or routed interfaces. For more detailed command references of all the IPv6 ND features, visit the IPv6 Command Reference Page by clicking here.

Router Advertisement (RA)

IPv6 Routers periodically advertise their presence to other nodes by sending RA packets. Run the command below to enable RA on a layer 3 interface.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd suppress-ra false
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd suppress-ra false
admin@Xorplus# commit
```

Router Advertisement Interval

To set the RA interval, run the command below. RA interval can be set in milliseconds or in seconds. The example below sets the RA interval to 1000 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-interval sec 1000
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd ra-interval sec 1000
admin@Xorplus# commit
```

RA Fast Retransmit

According to RFC4861 consecutive RA packets should be sent with at least 3 seconds delay. PICOS by default bypasses this restriction by fast transmission of RA to achieve better convergence. Run the command below enable or disable this feature. Default is enabled.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-fast-retrans false
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd ra-fast-retrans false
admin@Xorplus# commit
```

Default Router Preference

Routers may include the default router preference in RA packets to signal to nodes the router preference in *low, medium* or *high.* Router preference is send using the unused bits in the RA packet. The hosts that do not implement the default router preference will ignore these bits. The command below sets the default router preference to low.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd router-preference low
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd router-preference low
admin@Xorplus# commit
```

Advertisement Interval Option

The Advertisement Interval Option indicates to host the maximum time in milliseconds between successive unsolicited Router Advertisements. Run the command below to set this option.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd adv-interval-option
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd adv-interval-option
admin@Xorplus# commit
```

Home Agent Option

The Home Agent Option flag can be set or unset in IPv6 RA packets and is used to indicate to hosts that the router acts as Home Agent and includes a Home Agent Option. This option is not set by default. Run the command below to set this option.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-config-flag
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd home-agent-config-flag
admin@Xorplus# commit
```

Home Agent Lifetime

This parameter specifies the value to be place in Home Agent Option when its set. The default value is 0 which means the current Router Lifetime value. The command below sets the Home Agent Lifetime to 5 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-lifetime 5
admin@Xorplus# commit
```

or

```
admin@XorPlus# set l3-interface routed-interface rif-ge3 ipv6-nd home-agent-lifetime 5
admin@Xorplus# commit
```

PICOS L2/L3 Support for IPv6

Please note that the N22XX series switches do not support IPv6.

Since PICOS version 4.1.0, the following protocols are protocol components supports IPv6.

- VRRPv3
- BGPv3
- OSPFv3
- DHCP Relay
- RIPng

The following System related features offer support for IPv6.

- Syslog
- NTP
- TACACS

Enable Path MTU Discovery

Overview

The Path MTU (PMTU) discovery protocol dynamically discovers the MTU value of each hop along a given transmission path, which saves IPv6 device processing resources and helps IPv6 networks run more efficiently.

The PMTU protocol is accomplished through the Packet Too Big message of ICMPv6. The basic idea is that a source node initially assumes that the PMTU of a path is the MTU of its outgoing interface. If any of the IPv6 packets sent on that path are too large to be forwarded by some node along the path, that node will discard them and return ICMPv6 Packet Too Big messages to the source node with its own MTU value.

Upon receipt of such a message, the source node reduces its assumed PMTU for the path based on the MTU of the constricting hop as reported in the Packet Too Big message. The decreased PMTU causes the source to send smaller packets. This process is repeated until the message reaches the destination, then the source node knows the minimum MTU in the path of two communicating hosts which is called the Path MTU value.

The PMTU of a path may change over time, due to changes in the routing topology. Reductions of the PMTU are detected by Packet Too Big messages. To detect increases in a path's PMTU, a node periodically restores its assumed PMTU to the originally configured MTU value of the system (configured by using command **set l3-interface vlan-interface** <*interface-name*> **mtu** <*mtu-value*> or **set l3-interface routed-interface** <*interface-name*> **mtu** <*mtu-value*>).

NOTE:

- Although the PMTU value is triggered by the IPv6 packets, once generated, it controls the size of both the IPv4 and IPv6 packets forwarded.
- The PMTU value takes effect only to the packets in the outgoing direction of the interface.

Enabling Path MTU Discovery

The following commands can be used to enable or disable PMTU function on a VLAN interface or a routed interface.

set l3-interface vlan-interface <*vlan-interface*> **pmtu-discovery disable** <**true | false**>

set l3-interface routed-interface <*routed-interface*> **pmtu-discovery disable** <**true | false**>

Enable PMTU function on all the nodes in the path where you want to apply the PMTU function.

- The following example enables PMTU function on VLAN interface *vlan100*.

```
admin@PICOS# set l3-interface vlan-interface vlan100 pmtu-discovery disable falseadmin@PICOS# commit
```

- The following example enables PMTU function on routed interface *rif-te19*.

```
admin@PICOS# set l3-interface routed-interface rif-te19 pmtu-discovery disable false
admin@PICOS# commit
```

IPv6 Neighbor Discovery Inspection

- Overview of ND Inspection
- Configuring ND Inspection
- Example for ND Inspection

Overview of ND Inspection

- Terminology
  - Neighbor Solicitation (NS)
  - Neighbor Advertisement (NA)
  - Router Solicitation (RS)
  - Router Advertisement (RA)
  - Redirect (RR)
  - DHCPv6 Snooping
  - Duplicate Address Detection (DAD)
  - ND Inspection Trusted port
  - ND Inspection Untrusted port
- ND Inspection Operation Mechanism
  - Binding Entry Check
  - Source MAC Address Validation

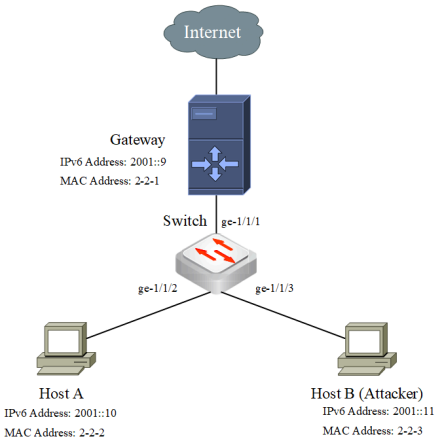
IPv6 Neighbor Discovery (ND) Inspection mitigates NDP security vulnerability by checking detailed information of message and verifying them against DHCPv6 snooping binding table or neighbor discovery snooping binding table.

The detailed information referred to the following points:

The HostB (Attacker) spoofs the IPv6 address of the victim's (Host A) by sending NS/NA/RS messages. As a result, the gateway and other hosts update the neighbor incorrect address information. All messages intended for the victim are sent to the attacking terminal.

The HostB (Attacker) spoofs the gateway by sending NA messages. As a result, all hosts attached to the victim gateway maintain an incorrect IPv6 configuration.

Figure 1. ND Attack Diagram



Terminology

Neighbor Solicitation (NS)

IPv6 nodes (a host or network device using IPv6 protocol) send NS messages primarily to get the link-layer addresses of their neighbors and detect neighbor reachability and duplicate addresses.

Neighbor Advertisement (NA)

IPv6 hosts respond to NS messages by sending. Additionally, IPv6 nodes, including hosts and network devices, send NA messages when the link-layer topology changes.

Router Solicitation (RS)

When an IPv6 node starts, it sends an RS packet to a router to request prefixes and other essential configuration details. It then waits for RA packet from the router in response.

Router Advertisement (RA)

A router periodically advertises RA messages, including network configurations such as network prefix to IPv6 nodes. The router also returns RA messages as the responses to RS messages.

Redirect (RR)

When detecting that the inbound interface and outbound interface of a packet are the same, a router sends a Redirect message to request the IPv6 node to select a better next hop address.

DHCPv6 Snooping

DHCPv6 snooping is a security feature that establishes DHCPv6 snooping binding table to record client information by capturing messages between server and client. DHCP snooping creates a binding table, which includes the client IP address, MAC address, VLAN ID, physical port and the lease time.

Duplicate Address Detection (DAD)

In an IPv6 network, when an interface attempts to configure a unicast IPv6 address, it first performs DAD to ensure that the address is unique on the link.

The purpose of DAD is to prevent address conflicts and ensure smooth network communication.

ND Inspection Trusted port

This type of port is used to connect to trusted IPv6 nodes. After the user configures the port as a trusted port, the device will no longer check NS/NA/RS/RA messages in the table entries.

ND Inspection Untrusted port

All ports are untrusted by default without modifying port properties.

ND Inspection Operation Mechanism

ND inspection is mainly for filtering illegal messages, the forged ND message has the following characteristics:

The source MAC address and the MAC address in the source link layer address in the forged ND message do not match.

The mapping relationship between the source IPv6 address and the source MAC address in the forged ND message is not real for the legal user.

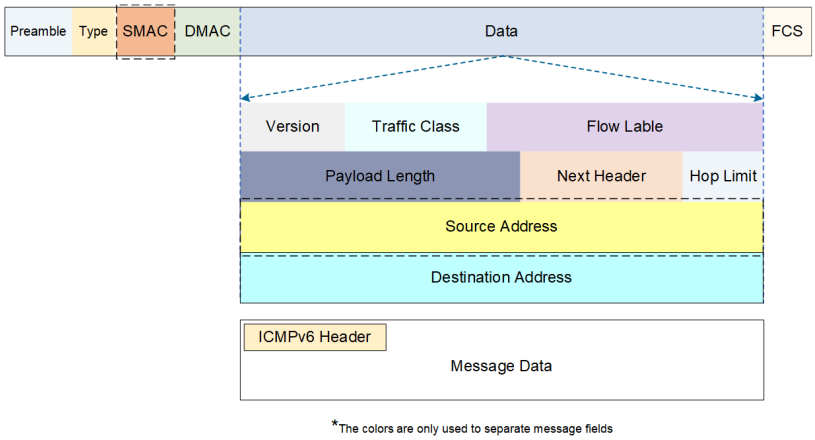
According to the characteristics of the attack messages, the device can check ND messages to effectively prevent ND attacks.

Binding Entry Check

With ND inspection enabled, after a device receives an ND message, the device will verify the NS/NA/RS/RA message with the DHCPv6 snooping table entry already generated.

Verify if the source MAC address and source IP address exists in ND message, if the ND message fields match with the source IPv6 address and source MAC address in the table, the device will consider ND message is legal and forward the message. Otherwise, the device discards the message.

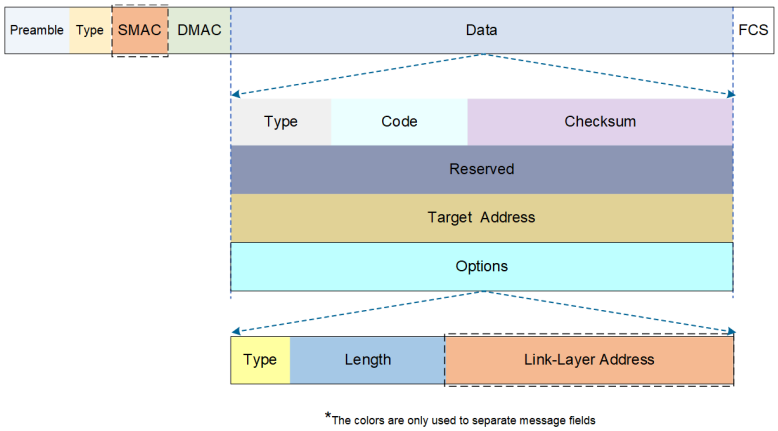
Figure 2. IPv6 Message Diagram



Source MAC Address Validation

After configuring source MAC address validation, the device will check if the source MAC address in the ND message is consistent with the Link-Layer Address (for example: 22:22:22: 22:22:21), if they are not the same, the device will discard the message. The diagram is shown below.

Figure 3. ND Message Diagram



If the user specifies a trusted port, the system will no longer check the ND message and directly forward the message, but still check source MAC consistency.

Configuring ND Inspection

Step 1 Enable DHCPv6 snooping.

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

NOTE:

ND inspection does not generate table entries by itself and needs to rely on the table entries formed by DHCPv6 snooping, thus, user needs to enable DHCPv6 snooping first.

Step 2 Enable ND inspection for a VLAN.

set protocols neighbour inspection vlan <*vlan-id*> **disable** <**true** | **false**>

NOTE:

DAD message does not carry a source MAC address; therefore, this type of message will be skipped in ND inspection.

Step 3 (Optional) Configure the device to check source MAC address against the link-layer source address.

set protocols neighbour inspection validate source-mac

Step 4 (Optional) Configure the trust-port for a device.

set protocols neighbour inspection trust-port <*port*>

Step 5 Commit the configurations.

commit

Step 6 View DHCPv6 snooping dynamic binding table entries used by ND inspection.

run show nd inspection dhcp6-snooping binding

Example for ND Inspection

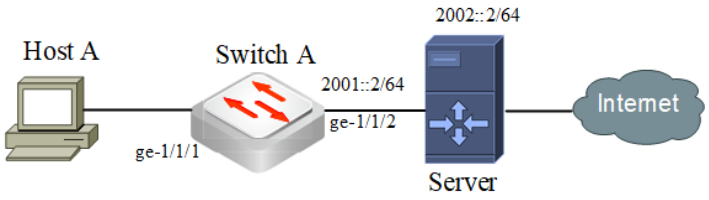
- Networking Requirements
- Procedure
  - Switch A
  - Verifying the Configuration

Networking Requirements

Building the corresponding network according to the topology diagram, and do the basic network connectivity configuration, configure the ND snooping inspection feature on Switch A, and after the correct configuration is completed, check the effective configuration on Switch A.

Host A accesses the DHCPv6 Server through Switch A and Switch A forwards the IPv6 address assigned by the DHCPv6 Server to Host A.

Figure 1. ND Inspection Configuration Example



Procedure

Switch A

Step 1 Add VLAN members to trunk ports.

```
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 20
```

Step 2 Enable DHCPv6 snooping.

```
admin@SwitchA# set protocols dhcp6 snooping trust-port ge-1/1/2
admin@SwitchA# set protocols dhcp6 snooping vlan 20 disable false
admin@SwitchA# set protocols dhcp6 traceoptions flag all disable false
```

Step 3 Enable ND inspection and verify source MAC address.

```
admin@SwitchA# set protocols neighbour inspection vlan 20 disable false
admin@SwitchA# set protocols neighbour inspection trust-port ge-1/1/2
admin@SwitchA# set protocols neighbour inspection validate source-mac
```

Step 4 Commit the configurations.

```
admin@ SwitchA # commit
```

Verifying the Configuration

The show command can be used to show table entry about configuration on Switch A.

The **run show dhcp6 snooping binding** command is used to view DHCPv6 snooping binding table.

The **run show nd inspection dhcp6-snooping binding** command is used to view DHCPv6 snooping dynamic binding table entries used by ND inspection..

- View DHCPv6 snooping binding table.

```
admin@ Switch A# run show dhcp6 snooping binding
Total Snooping host count:     1
MAC Address        IPv6 Address     Port   VLAN ID   Lease(sec)
-------------------------------------------------------------------

22:22:22: 22:22:22   2001::1        ge-1/1/1   20       63/120
```

- View DHCPv6 snooping dynamic binding table entries used by ND inspection.

```
admin@ Switch A # run show nd inspection dhcp6-snooping binding
Valid Dhcp6 Snooping host count:     1
VLAN ID                 IPv6 Address             MAC Address
-------------------------------------------------------------------
20                      2001::1                  22:22:22: 22:22:22
```

IPv6 Neighbor Discovery Snooping

- Overview of ND Snooping
- Operation Mechanism of ND Snooping
- Configuring ND Snooping
- Example for ND Snooping

Overview of ND Snooping

- Terminology
  - IPv6 ND
  - Neighbor Solicitation (NS)
  - Neighbor Advertisement (NA)
  - Router Solicitation (RS)
  - Router Advertisement (RA)
  - Duplicate Address Detection (DAD)
  - Redirect (RR)
  - ND Snooping Trusted Port
  - ND Snooping Untrusted port
- ND Attacks
  - Address Spoofing Attack
  - RA Attack

The IPv6 ND (Neighbor Discovery) protocol is a key protocol in IPv6 networks that combines and enhances the ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol) route discovery, and ICMP redirection protocols of IPv4. The ND protocol plays a critical role in IPv6 networks, providing several important functions to ensure that devices in the network can communicate with each other and maintain network stability.

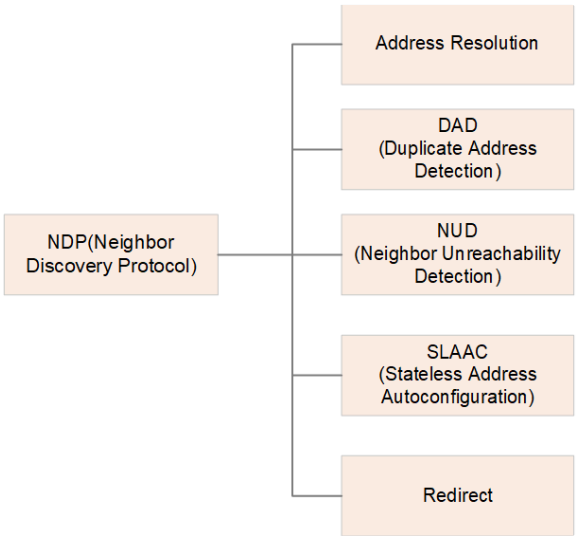
The IPv6 ND protocol is powerful but does not have a relevant security mechanism. ND snooping is a security feature for IPv6 ND, which allows users to configure the port type. The port will capture messages from the corresponding ports and generate prefix management or dynamic binding tables to defend against ND attacks from bogus hosts or gateways.

Terminology

IPv6 ND

The ND protocol is a key protocol for IPv6, which combines the protocols of ARP, ICMP route discovery, and ICMP redirection from IPv4 and improves them. As a fundamental protocol for IPv6, ND provides multiple functions as show in the following figure.

Figure 1. Neighbor Discovery Protocol Function Diagram



Neighbor Solicitation (NS)

IPv6 nodes (hosts or network devices using the IPv6 protocol) can get the link-layer addresses of their neighbors through NS messages to check whether the neighbors are reachable or not, and they can also perform DAD (Duplicate Address Detect).

Neighbor Advertisement (NA)

IPv6 hosts respond to NS message by sending NA packets. Additionally, IPv6 nodes, including hosts and network devices, send NA message when the link-layer topology changes.

Router Solicitation (RS)

Upon starting, an IPv6 node sends an RS message to a router to request prefixes and other essential configuration details. It waits for a RA message from the router in response.

Router Advertisement (RA)

A router periodically advertises RA message, including network configurations such as network prefix to IPv6 nodes. The router also returns RA message as the responses to RS message.

Duplicate Address Detection (DAD)

In an IPv6 network, when an interface attempts to configure a unicast IPv6 address, it first performs DAD to ensure that the address is unique on the link.

The purpose of DAD is to prevent address conflicts and ensure smooth network communication.

Redirect (RR)

When detecting that the inbound interface and outbound interface of a packet are the same, a router sends a redirect packet to request the IPv6 node to select a better next hop address.

ND Snooping Trusted Port

This type of port is used to connect to trusted IPv6 nodes, for ND messages received from this type of port, the device forwards them normally, and at the same time, the device will build a prefix management table based on the received RA messages.

Users can execute `set protocols neighbour snooping trust-port` command to specify ports connected to IPv6 nodes into trusted ports. By default, all ports of the device are untrusted

ND Snooping Untrusted port

This type of port is used to connect untrusted IPv6 nodes, and the device considers RA messages received from this type of port as illegal messages and directly discards them.

ND protocol provides powerful functions, but it is easier to be utilized by the attacker for its weaker security mechanism, ND protocol attacks include the following types.

ND Attacks

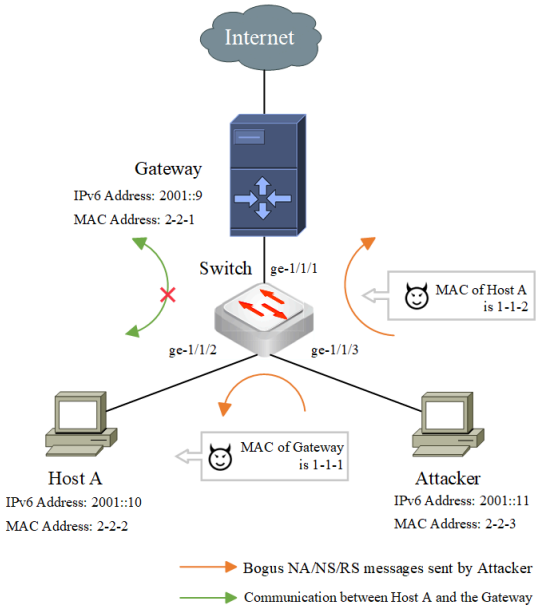
ND protocol provides powerful functions, but it is easier to be utilized by the attacker for its weaker security mechanism, ND protocol attacks include the following types.

Address Spoofing Attack

Attacker uses the IP of Host A and sends NA/NS/RS message to the gateway, which modifies the ND entries of the gateway and records the incorrect entries of Host A. The attacker easily gets the data that the gateway communicates with Host A.

Attacker uses the IP of gateway and sends forged NA/NS/RS message to Host A, Host A records wrong entry. As a result, Host A cannot receive message from the gateway, Host A and the gateway cannot communicate with each other, and the attacker can easily get the data that intended to be sent to the gateway.

Figure 2. Address Spoofing Attack

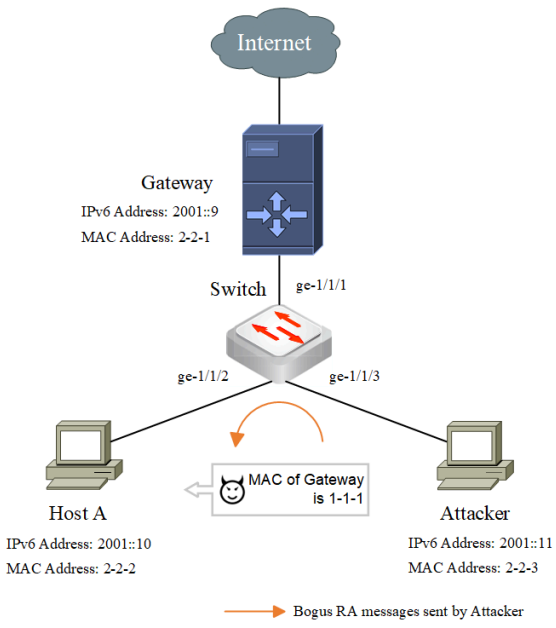


RA Attack

Attacker sends forged RA messages.

- Forges non-existent prefixes, modifies Host A's routing table.
- Forges the gateway's MAC and router lifetime, modifies the host's default gateway.
- Forges the DHCP server, and at the same time, forges the flag bit in the RA message, which made Host A being assigned a false address using the DHCP server.

Figure 3. RA Attack



In summary, getting the real IPv6 address-MAC of the device and filtering out the illegal ND messages are the keys to solve the anti-attack of the ND protocol. ND snooping is proposed at this point. This feature enables the filtering of illegal messages by checking the fields of

the established table entries. For a detailed description, please refer to Operation Mechanism of ND Snooping

Operation Mechanism of ND Snooping

- Prefix Management Table
  - Entry Creation and Update Mechanism of Prefix Management Table
  - Aging Mechanism of Prefix Management Table Entries
- ND Snooping Dynamic Binding Table
  - Entry Creation and Update Mechanism of Dynamic Binding Table
    - Receiving DAD Messages
    - Receiving NS or RS Messages
    - Receiving NA Messages
  - Aging Mechanism of Dynamic Binding Table Entries

Prefix Management Table

After enabled the ND snooping, the device captures RA messages sent from the trusted port and generates a prefix management table. An entry includes information about prefix, prefix length, port, VLAN ID, valid- time, prefix-type.

Entry Creation and Update Mechanism of Prefix Management Table

After ND snooping is enabled, a trusted port receives an RA message and checks whether the prefix of the message exists.

- If the prefix does not exist, the system creates a new prefix management table entry.
- If the prefix exists, the device updates the entries according to the RA message and forwards.

When the untrusted port receives a RA message, it will discard the message. If the port receives the NS/NA/RS message, it will process the entries then decide forward or not.

Aging Mechanism of Prefix Management Table Entries

When the valid time in the prefix table expires, the entry will be deleted.

ND Snooping Dynamic Binding Table

After ND snooping enabled, the device establishes the ND snooping dynamic binding table, and the device can filter spoofed messages by checking NA, NS, and RS messages against dynamic binding table entry. An entry includes information about IPv6 address, MAC address, input port, VLAN ID, lease.

Entry Creation and Update Mechanism of Dynamic Binding Table

After ND snooping enabled, the device receives a DAD NS message, it will check whether there is a corresponding prefix management table entry based on the Target Address.

The creation and update mechanism of the dynamic binding table in ND snooping is as follows:

Receiving DAD Messages

If entry does not exist, the message will be discarded.

If the entry exists, it then checks whether there is a ND snooping dynamic binding table entry based on Target Address.

> **NOTE:**
>
> The Target Address cannot be a multicast address.

- If no such entry exists, the device creates a new ND snooping dynamic binding table entry and forwards the message.

- If the entry exists, the device checks whether the source MAC address, input port, and VLAN of the DAD NS message are the same with the entry.
  - If they are consistent, it updates the address lease of the corresponding entry.
  - If the MAC addresses are consistent but other information is not, it updates other fields in the entry and forwards the message.
  - If the MAC addresses are different, the device retains the entry and forwards the message.

Receiving NS or RS Messages

When the device receives a common NS or RS message, it checks if there is a corresponding dynamic binding entry based on source IP address. If no such entry exists, the message will be discarded. If an entry exists, the device checks if the MAC address, input port, and VLAN of the NS/RS message are the same with the entry.

- If all the information is consistent, the device updates lease.
- If the information is different, the device discards the message.

Receiving NA Messages

When the device receives a NA message, it checks if there is a corresponding dynamic binding entry based on source IP address. If no such entry exists, the NA message will be discarded. If an entry exists, the device then checks if the MAC address, port, and VLAN in the NA message are the same.

- If all the information is same, the device will update lease.
- If the MAC address is the same but other information are not, the device will update data and forward the message.
- If the MAC address is different, the device discards the message.

Aging Mechanism of Dynamic Binding Table Entries

If the lease time of a user address expires, the table entry ages automatically.

When the device receives a new or updated entry from NS message, the detailed description is as follows.

If it receives a response NA message notifying that the user's address has been used from other users within a certain period, the device will delete the entry.

If the device receives a response NA message notifying that the user's address has been used from other users beyond this period, the device does not delete the entry.

Configuring ND Snooping

Step 1 Enable ND snooping protocol in corresponding VLAN.

set protocols neighbour snooping vlan <*vlan-id*> **enable true**

Step 2 ND snooping classifies ports connected to IPv6 nodes into trusted and untrusted ports. By default, all ports of the device are untrusted.

set protocols neighbour snooping trust-port <*port*>

> **NOTE:**
>
> `<port>` can be a valid physical port or a LAG (Link Aggregation Group) port. The members of the LAG port don't support configuration as a trust port.

Step 3 (Optional) Configure the maximum number of ND snooping dynamic binding table entries a device is allowed to learn.

set protocols neighbour snooping max-user-number <*max-user-num*>

Step 4 (Optional) If the device does not send RA messages, the prefix management table entries cannot automatically generate, in this scenario, user can configure static prefix.

set protocols neighbour snooping static-prefix <*IPv6Net*> **vlan** <*vlan-id*>

> **NOTES:**
>
> - `<IPv6Net>` cannot be ::/0, multicast address.
> - `<vlan-id>` must be configured when add or delete.

Step 5 Commit the configuration.

commit

Step 6 View the configuration information and table entries about ND snooping.

run show neighbor snooping

run show neighbor snooping prefix [static | dynamic]

run show neighbor snooping binding

Step 7 (Optional) If needed, users can clear the entries of ND snooping.

run clear neighbor snooping prefix

run clear neighbor snooping binding

Example for ND Snooping

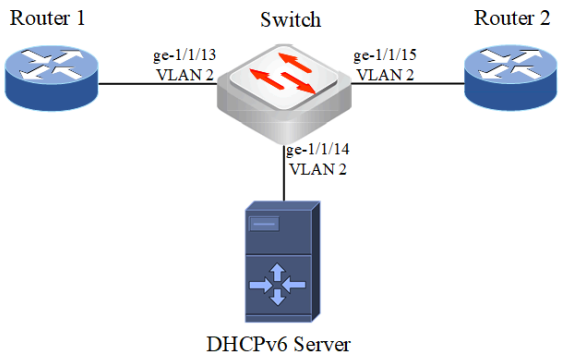
- Networking Requirements
- Procedure
  - Switch A
  - Verifying the Configuration

Networking Requirements

Building the corresponding network according to the topology diagram, and do the basic network connectivity configuration, configure the ND snooping function on Switch A, and after the correct configuration is completed, check the effective ND snooping binding table on Switch A.

- Router1 gets an IP address through SLAAC (Stateless Address Autoconfiguration).
- Router2 gets an IP through DHCP (Dynamic Host Configuration Protocol).

Figure 1. ND Snooping Configuration Example



Procedure

Switch A

Step 1 Add VLANs members to trunk ports.

```
admin@SwitchA# set interface gigabit-ethernet ge-1/1/13 family ethernet-switching native-vlan-id 2
admin@SwitchA# set interface gigabit-ethernet ge-1/1/13 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/13 family ethernet-switching vlan members 2
admin@SwitchA#set interface gigabit-ethernet ge-1/1/14 family ethernet-switching native-vlan-id 2
admin@SwitchA# set interface gigabit-ethernet ge-1/1/14 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/14 family ethernet-switching vlan members 2
admin@SwitchA# set interface gigabit-ethernet ge-1/1/15 family ethernet-switching native-vlan-id 2
admin@SwitchA# set interface gigabit-ethernet ge-1/1/15 family ethernet-switching port-mode trunk
admin@SwitchA# set interface gigabit-ethernet ge-1/1/15 family ethernet-switching vlan members 2
admin@SwitchA# set vlans vlan-id 2
```

Step 2 Configure ge-1/1/14 as trust port and enable ND snooping on VLAN 2.

```
admin@SwitchA# set protocols neighbour snooping vlan 2 enable true
admin@SwitchA# set protocols neighbour snooping trust-port ge-1/1/14
admin@SwitchA# set protocols neighbour traceoptions disable false
admin@SwitchA# set system log-level trace
```

Step 3 Commit the configurations.

```
admin@ SwitchA # commit
```

Verifying the Configuration

The **run show neighbor snooping binding** command is used to view ND snooping dynamic management table entries on Switch A.

The **run show neighbor snooping prefix** command is used to view ND snooping prefix management table entries on Switch A.

The **run show neighbor snooping** command is used to view ND snooping configuration on Switch A.

- View ND snooping dynamic management table entries.

```
admin@SwitchA # run show neighbor snooping binding
Total Snooping binding count:     2
MAC Address     IPv6 Address       Port     VLAN ID   Status     Lease(sec)
-------------------------------------------------------------------------------
dc:b:9:65:6f:f7  3000::de0b:9ff:fe65:6ff7  ge-1/1/13   2      Valid      48/120
dc:b:9:65:6f:f7  fe80::de0b:9ff:fe65:6ff7  ge-1/1/13   2      Valid      27/120
```

- View ND snooping prefix management table entries.

```
admin@ SwitchA # run show neighbor snooping prefix
Total Snooping table prefix count:    1
Total Snooping table dynamic count:  1
Total Snooping table static count:     0
Prefix          Length     Port       VLAN ID   Valid-Time    Prefix-Type
-------------------------------------------------------------------------------
3000::          64       ge-1/1/14      2        48/120       Dynamic
```

- View ND snooping configuration.

```
admin SwitchA # run show neighbor snooping
ND Snooping enabled vlans: 1
ND Snooping trust-ports: ge-1/1/14
ND Snooping max-user-number: 9216
```

VRF Route Leaking Configuration

Generally speaking, multiple VRFs maintain separate routing tables that are independent of each other. But there are scenarios where a specific destination is only reachable from a specific VRF. For example, a DHCP server in one VRF can only be accessible to hosts in that VRF. If clients in other VRFs want to access this DHCP server, we need to have a mechanism where we can have a route in one VRF for which the destination next-hop address is located in a different VRF.

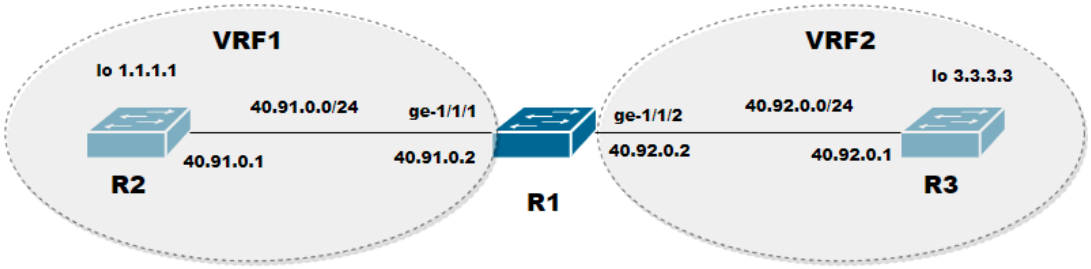


Figure 1. VRF Route Leaking Example

As shown in Figure 1, if hosts attached to R1 in VRF1 wants to access resources located in VRF2 and accessible through R3, we will need to enable route leaking between VRF1 and VRF2. From the topology above, R1 has two interfaces, one each in VRF1 and VRF2. For resources in VRF2 to be accessible to hosts in VRF1, routes in VRF2 needs to be leaked into VRF1.

Leaked routes once configured on a device can be distributed to neighboring devices through either BGP or OSPF. If a leaked route is a BGP route then it will be dynamically replicated from source to destination VRF by BGP. If the route to be leaked is a non-BGP route, then that route first needs to be redistributed into BGP before it can be leaked to the destination VRF.

Route leaking can be used to reach directly connected hosts in the source VRF as well as reach remote destinations accessible through the source VRF. In Figure 1, the leak will be configured on R1. For the loopback interface 1.1.1.1 on R2 in VRF1, to ping loopback interface 3.3.3.3 on R3 in VRF2, R1 device will need two routes in both VRF1 and VRF2. On R1, the route to reach 3.3.3.3 in VRF2 is **3.3.3.3/32 next-hop 40.92.0.1**. Similarly, to reach 1.1.1.1 the route in VRF2 will be **1.1.1.1 next-hop 40.91.0.2 next-hop vrf vrf1.** VRF2 does not have a route for loopback 1.1.1.1 in VRF2 hence apart from specifying the next-hop address of 40.91.0.1, the route must also specify the next-hop VRF which in this case is VRF1. Similarly, there are also two routes in VRF1. The two routes in VRF1 on R1 are, **1.1.1.1/32 next-hop 40.91.0.1** and **3.3.3.3/32 next-hop 40.92.0.1 next-hop vrf vrf2.**

In PICOS, there is no restriction on leaking routes to and from the default VRF. Routes can be leaked from the default VRF into any user defined VRF and vice versa.

Route Leaking Limitation

1. Directly connected subnets or hosts are not allowed to be leaked from one VRF into another. In Figure 1, for example, subnet 40.92.0.0/24 in VRF 2 cannot be leaked into VRF 1 on R1.
2. On R3 switch, all routes in VRF2 can be leaked into VRF1 by configuring route leaking on R1 except the subnets directly connected with R1, for example in this case, subnet 40.92.0.0/24 cannot be leaked into VRF1.
3. Overlapping addresses in two VRFs are not allowed when enabling route leaking between these two VRFs. It is thus strongly recommended to use non-overlapping addresses in different VRFs before implementing route leaking.
4. VRF route leaking doesn't work in case of VXLAN routing. The routes cannot be leaked to a VRF corresponding to an VXLAN instance.
5. The configuration of route leaking by importing BGP IPv4 routes from one user-defined VRF into another user-defined VRF, for example:

   set protocols bgp vrf vrf1 local-as 1
   set protocols bgp vrf vrf1 ipv4-unicast import vrf vrf2
   set protocols bgp vrf vrf2 local-as 2
   This will cause configuration from PICOS CLI is not consistent with FRR configuration. Specifically, FRR will add "set protocols bgp local-as 1" (local as number is same as the value in vrf1) to its configuration automatically, which is not in PICOS CLI. From version 4.4.0, if "set protocols bgp local-as 1" is not configured, the above configurations are not allowed.

BGP Route Leaking Configuration Example

This document illustrates dynamic route leaking between different VRFs. There are three switches in our example topology as shown in Figure 1.

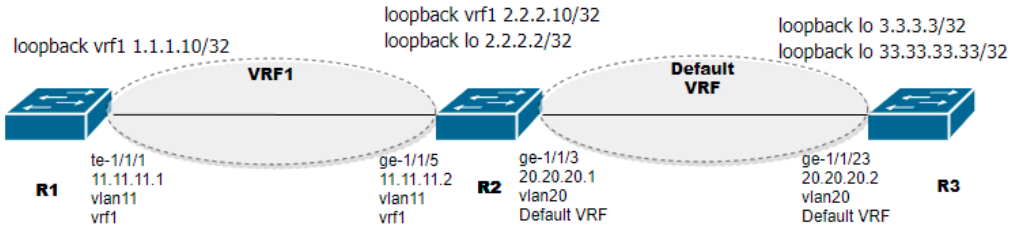


Figure 1. Dynamic Route Leaking Example Topology

Topology Introduction

- OSPFv2 is configured between devices R1 and R2. The interfaces connecting these two devices both belong to VRF1.
- BGP is configured between devices R2 and R3. The interfaces connecting these two devices both belong to the default VRF.
- Dynamic route leaking using BGP is configured on R2.
- On R2, BGP routes in the default VRF are leaked into VRF1. The BGP routes are then redistributed into OSPF in VRF1.
- Similarly, on R2, BGP routes in VRF1 are leaked into the default VRF.
- On R2, OSPF routes in VRF1 are redistributed into BGP.
- Route map is used on R2 to demonstrate route filtering when leaking routes between the two VRFs.

Router Configuration

This section describes the configuration used on the three devices.

R1 Configuration

Step 1. Configure physical interfaces, L3 VLAN interfaces and IP addressing.

```
root@R1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode "trunk"
root@R1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 11
root@R1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching port-mode "trunk"
root@R1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching vlan members 101
root@R1# set l3-interface vlan-interface vlan101 address 101.101.101.1 prefix-length 24
root@R1# set l3-interface vlan-interface vlan11 address 11.11.11.1 prefix-length 24
root@R1# set vlans vlan-id 11 l3-interface "vlan11"
root@R1# set vlans vlan-id 101 l3-interface "vlan101"
```

Step 2. Create vrf1 and assign vlan11 and vlan101 to vrf1 and enable IP routing on the device.

```
root@R1# set ip vrf vrf1
root@R1# set l3-interface vlan-interface vlan11 vrf "vrf1"
root@R1# set l3-interface vlan-interface vlan101 vrf "vrf1"
root@R1# set ip routing enable true
```

Step 3. Create a loopback interface in vrf1 and set system hostname.

```
root@R1# set l3-interface loopback vrf1 address 1.1.1.10 prefix-length 32
root@R1# set system hostname R1
```

Step 4. Configure OSPFv2 by setting router ID and enable OSPF for different network prefixes.

```
root@R1# set protocols ospf vrf vrf1 router-id 1.1.1.10
root@R1# set protocols ospf vrf vrf1 network 101.101.101.0/24 area "0"
root@R1# set protocols ospf vrf vrf1 network 11.11.11.0/24 area "0"
```

```
root@R1# set protocols ospf vrf vrf1 network 1.1.1.10/32 area "0.0.0.0"
```

R2 Configuration

Step 1. Configure physical interfaces, L3 VLAN interfaces and IP addressing.

```
root@R2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 20
root@R2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode "trunk"
root@R2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 11
root@R2# set l3-interface vlan-interface vlan11 address 11.11.11.2 prefix-length 24
root@R2# set l3-interface vlan-interface vlan20 address 20.20.20.1 prefix-length 24
root@R2# set vlans vlan-id 11 l3-interface "vlan11"
root@R2# set vlans vlan-id 20 l3-interface "vlan20"
```

Step 2. Create vrf1 and assign vlan11 to vrf1 and enable IP routing on the device.

```
root@R2# set ip routing enable true
root@R2# set ip vrf vrf1
root@R2# set l3-interface vlan-interface vlan11 vrf "vrf1"
```

Step 3. Create loopback interfaces in the default VRF and vrf1 and set the system hostname.

```
root@R2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
root@R2# set l3-interface loopback vrf1 address 2.2.2.10 prefix-length 32
root@R2# set system hostname R2
```

Step 4. Configure OSPFv2 by setting router ID and enable OSPF for different network prefixes. Also enable redistribution of BGP routes into OSPFv2.

```
root@R2# set protocols ospf vrf vrf1 router-id 2.2.2.10
root@R2# set protocols ospf vrf vrf1 network 11.11.11.0/24 area "0"
root@R2# set protocols ospf vrf vrf1 network 21.21.21.0/24 area "0"
root@R2# set protocols ospf vrf vrf1 redistribute bgp
```

Step 5. Configure BGP by setting router ID, specify BGP neighbor, AS number and enable route leaking by importing routes into VRF1 from the default VRF.

```
root@R2# set protocols bgp local-as 200
root@R2# set protocols bgp router-id 2.2.2.2
root@R2# set protocols bgp neighbor 20.20.20.2 remote-as "300"
root@R2# set protocols bgp ipv4-unicast network 2.2.2.2/32
root@R2# set protocols bgp ipv4-unicast import vrf vrf1
root@R2# set protocols bgp vrf vrf1 local-as 201
root@R2# set protocols bgp vrf vrf1 router-id 2.2.2.2
root@R2# set protocols bgp vrf vrf1 ipv4-unicast redistribute ospf
root@R2# set protocols bgp vrf vrf1 ipv4-unicast import vrf default
```

Step 6. Configure route map *map1* to filter route 33.33.33.33/32 and only leak 3.3.3.3/32 into VRF1.

```
root@R2# set routing prefix-list ipv4-family pre1 seq 1 permit prefix 3.3.3.3/32
root@R2# set routing route-map map1 order 1 matching-policy "permit"
root@R2# set routing route-map map1 order 1 match ipv4-addr address prefix-list "pre1"
root@R2# set protocols bgp vrf vrf1 ipv4-unicast import vrf-route-map "map1"
```

R3 Configuration

Step 1. Configure physical interfaces, L3 VLAN interfaces and IP addressing.

```
admin@R3# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching native-vlan-id 200
admin@R3# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching port-mode trunk
admin@R3#set interface gigabit-ethernet ge-1/1/10 family ethernet-switching vlan members 201
admin@R3# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 20
admin@R3# set l3-interface vlan-interface vlan20 address 20.20.20.2 prefix-length 24
admin@R3# set l3-interface vlan-interface vlan200 address 200.200.200.1 prefix-length 24
admin@R3# set vlans vlan-id 20 l3-interface vlan20
admin@R3# set vlans vlan-id 200 l3-interface vlan200
admin@R3# set vlans vlan-id 201 l3-interface vlan201
```

Step 2. Enable IP routing on the device and create vrf1.

```
admin@R3# set ip routing enable true
admin@R3# set ip vrf vrf1
```

Step 3. Create loopback interfaces and set system hostname.

```
admin@R3# set l3-interface loopback lo address 3.3.3.3 prefix-length 32
admin@R3# set l3-interface loopback lo address 33.33.33.33 prefix-length 32
admin@R3# set system hostname R3
```

Step 4. Configure BGP AS number, router ID and add network prefixes.

```
admin@R3# set protocols bgp local-as 300
admin@R3# set protocols bgp router-id 3.3.3.3
admin@R3# set protocols bgp neighbor 20.20.20.1 remote-as "200"
admin@R3# set protocols bgp ipv4-unicast network 33.33.33.33/32
admin@R3# set protocols bgp ipv4-unicast network 3.3.3.3/32
```

Verify Configuration

R1 Routing Table

The command below shows the routing table of vrf1. As you can notice, route 33.33.33.33/32 is not leaked and redistributed into VRF1 because this prefix was filtered out by route map.

```
root@R1# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (blackhole), 01:08:45
O   1.1.1.10/32 [110/0] is directly connected, vrf1, weight 1, 01:08:44
C>* 1.1.1.10/32 is directly connected, vrf1, 01:08:45
O>* 3.3.3.3/32 [110/20] via 11.11.11.2, vlan11, weight 1, 00:33:58
O   11.11.11.0/24 [110/10] is directly connected, vlan11, weight 1, 01:06:36
C>* 11.11.11.0/24 is directly connected, vlan11, 01:07:17
O   101.101.101.0/24 [110/10] is directly connected, vlan101, weight 1, 01:07:44
C>* 101.101.101.0/24 is directly connected, vlan101, 01:07:44
```

R2 Routing Table

The following show command displays the routing table of vrf1 on R2. Again, route 33.33.33.33/32 is not present in this routing table since it is filtered using route map.

```
root@R2# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (blackhole), 01:09:36
O>* 1.1.1.10/32 [110/10] via 11.11.11.1, vlan11, weight 1, 01:08:20
C>* 2.2.2.10/32 is directly connected, vrf1, 01:09:36
B>* 3.3.3.3/32 [200/0] via 20.20.20.2, vlan20 (vrf default), weight 1, 00:14:43
O   11.11.11.0/24 [110/10] is directly connected, vlan11, weight 1, 01:09:10
C>* 11.11.11.0/24 is directly connected, vlan11, 01:09:10
O>* 101.101.101.0/24 [110/20] via 11.11.11.1, vlan11, weight 1, 01:08:20
```

Routing table of the default VRF on R2 is show below. Prior to route map filtering, route 33.33.33.33/32 can be seen in the default VRF.

```
root@R2# run show route
show ip route
=============
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K * 0.0.0.0/0 [255/8192] unreachable (blackhole), 01:11:08
K>* 0.0.0.0/0 [2/0] via 10.10.51.1, eth0, 01:11:08
B>* 1.1.1.10/32 [200/10] via 11.11.11.1, vlan11 (vrf vrf1), weight 1, 01:09:52
C>* 2.2.2.2/32 is directly connected, lo, 01:11:08
B>* 3.3.3.3/32 [20/0] via 20.20.20.2, vlan20, weight 1, 00:37:23
C>* 10.10.51.0/24 is directly connected, eth0, 01:11:08
C>* 20.20.20.0/24 is directly connected, vlan20, 01:10:26
B>* 33.33.33.33/32 [20/0] via 20.20.20.2, vlan20, weight 1, 01:08:21
B>* 101.101.101.0/24 [200/20] via 11.11.11.1, vlan11 (vrf vrf1), weight 1, 01:09:52
```

R3 Routing Table

Routing table of default VRF on R3 is show below.

```
admin@R3# run show route
show ip route
=============
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K * 0.0.0.0/0 [255/8192] unreachable (blackhole), 01:12:59
K>* 0.0.0.0/0 [2/0] via 10.10.51.1, eth0, 01:13:06
B>* 1.1.1.10/32 [20/10] via 20.20.20.1, vlan20, weight 1, 01:10:01
B>* 2.2.2.2/32 [20/0] via 20.20.20.1, vlan20, weight 1, 01:10:01
C>* 3.3.3.3/32 is directly connected, lo, 01:12:41
C>* 10.10.51.0/24 is directly connected, eth0, 01:13:06
C>* 20.20.20.0/24 is directly connected, vlan20, 01:12:05
C>* 33.33.33.33/32 is directly connected, lo, 01:12:41
B>* 101.101.101.0/24 [20/20] via 20.20.20.1, vlan20, weight 1, 01:10:01
C>* 200.200.200.0/24 is directly connected, vlan200, 01:12:04
```

Static Route Leaking Example

This document explains PICOS static route leaking. As shown in Figure 1, three devices, R1, R2 and R3 participate in this static route leaking example. The goal is to allow hosts connected to R2 in the default VRF, access to hosts connected to R3 in vrf2. To achieve this, static leaks will be configured on R1, which has two interfaces in two different VRFs, vrf2 and the default VRF. The interface connecting R2 belongs to the default VRF and the interface connecting R3 belongs to vrf2.

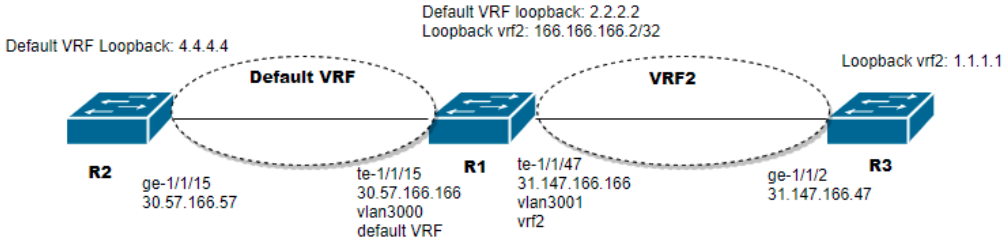


Figure1. Static Routing Leaking Topology

Static route leaks will be configured on R1. Additionally, a static route will be configured on R2 to reach 1.1.1.1 with a next-hop router address of R1 L3 VLAN interface. Similarly another static route will be configured on R3 to reach 4.4.4.4 with the next-hop router address of the R1 L3 VLAN interface. The sections below explains the device configuration of the three devices.

R1 Configuration

Step 1. Configure interface te-1/1/15 and te-1/1/47. Assign VLAN ID and configure the L3 VLAN interface IP address.

```
admin@R1# set interface gigabit-ethernet te-1/1/15 family ethernet-switching native-vlan-id 3000
admin@R1# set interface gigabit-ethernet te-1/1/47 family ethernet-switching native-vlan-id 3001
admin@R1# set l3-interface vlan-interface vlan3000 address 30.57.166.166 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan3001 address 31.147.166.166 prefix-length 24
admin@R1# set vlans vlan-id 3001 l3-interface "vlan3001"
admin@R1# set vlans vlan-id 3000 l3-interface "vlan3000"
admin@R1# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@R1# set l3-interface loopback vrf2 address 166.166.166.2
```

Step 2. Create VRF vrf2 and assign vlan3001 to vrf2. Also enable IP routing on the device.

```
admin@R1# set ip vrf vrf2
admin@R1# set l3-interface vlan-interface vlan3001 vrf "vrf2"
admin@R1# set ip routing enable true
```

Step 3. Create static leak routes on R1. Route 1.1.1.1/32 in created in the default VRF whereas route 4.4.4.4/32 is created in vrf2.

```
admin@R1# set protocols static route 1.1.1.1/32 nexthop-vrf vrf2 next-hop 31.147.166.47
admin@R1# set protocols static vrf vrf2 route 4.4.4.4/32 nexthop-vrf default next-hop 30.57.166.57
```

R2 Configuration

Step1. Configure interface ge-1/1/15, VLAN ID and L3 VLAN interface and IP address.

```
admin@R2# set interface gigabit-ethernet ge-1/1/15 family ethernet-switching native-vlan-id 3000
admin@R2# set l3-interface vlan-interface vlan3000 address 30.57.166.57 prefix-length 24
admin@R2# set vlans vlan-id 3000 l3-interface "vlan3000"
```

Step 2. Configure a static route to destination 1.1.1.1 and enable IP routing on the device. Also create the loopback interface and assign IP address.

```
admin@R2# set l3-interface loopback lo address 4.4.4.4 prefix-length 32
admin@R2# set protocols static route 1.1.1.1/32 next-hop 30.57.166.166
admin@R2# set ip routing enable true
```

R3 Configuration

Step1. Configure interface ge-1/1/2, L3 VLAN interface and IP address.

```
admin@R3# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3001
admin@R3# set l3-interface vlan-interface vlan3001 address 31.147.166.47 prefix-length 24
admin@R3# set vlans vlan-id 3001 l3-interface "vlan3001"
admin@R3# set l3-interface vlan-interface vlan3001 vrf vrf2
```

Step 2. Create vrf2, create loopback and configure a static route to destination 4.4.4.4/32 and also enable IP routing on the device.

```
admin@R3# set ip vrf vrf2
admin@R3# set l3-interface loopback vrf2 address 1.1.1.1 prefix-length 32
admin@R3# set protocols static vrf vrf2 route 4.4.4.4/32 next-hop 31.147.166.166
admin@R3# set ip routing enable true
```

Verify configuration

Ping 1.1.1.1 from R2 to test connectivity.

```
admin@R2# run ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=63 time=2.15 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=63 time=1.61 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=63 time=2.43 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=63 time=2.22 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=63 time=1.97 ms
```

Verify Routing Table on R1

```
admin@R1# run show route vrf vrf2
show ip route vrf vrf2 static
============================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf2:
S>* 4.4.4.4/32 [1/0] via 30.57.166.57, vlan3000 (vrf default), weight 1, 06:44:46
C>* 31.147.166.0/24 is directly connected, vlan3001, 00:31:25



show ipv6 route vrf vrf2 static
==============================

admin@R1# run show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 1.1.1.1/32 [1/0] via 31.147.166.47, vlan3001 (vrf vrf2), weight 1, 06:45:11
C>* 30.57.166.0/24 is directly connected, vlan3000, 00:51:25
```

Verify Routing Table on R2

```
admin@R2# run show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 1.1.1.1/32 [1/0] via 30.57.166.166, vlan3000, weight 1, 06:45:11
C>* 30.57.166.0/24 is directly connected, vlan3000, 00:51:25
```

Verify Routing Table on R3

```
admin@R3# run show route vrf vrf2
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

S>* 4.4.4.4/32 [1/0] via 31.147.166.166, vlan3001, weight 1, 06:45:11
C>* 31.147.166.0/24 is directly connected, vlan3001, 00:51:25
```

Bidirectional Forwarding Detection (BFD)

- Introduction of BFD
- Configuring BFD
  - Configuring Static BFD
  - Configuring Dynamic BFD
- Configuration Examples of BFD
  - Example for Configuring Single-Hop BFD
  - Example for Configuring Multi-Hop BFD
  - Example for Configuring BFD for BGP
  - Example for Configuring BFD for OSPF
  - Example for Configuring BFD for PIM-SM
- RFC Lists for BFD

Introduction of BFD

- Overview
- Single-Hop and Multi-Hop BFD
- BFD Working Process
- BFD Session Establishment
- Echo Function

Overview

Bidirectional Forwarding Detection (BFD) is a two-way forwarding detection mechanism, which can provide millisecond detection and realize the rapid detection of link faults.

Traditionally, the Hello message mechanism of routing protocols such as Open Shortest Path First (OSPF) and BGP has been used for link fault detection. The time required for this mechanism to detect a fault is in seconds. However, for high-speed data transmission, such as gigabit rate level, more than 1 second detection time will lead to a large amount of data loss; for delay-sensitive services, such as voice services, more than 1 second delay is unacceptable. BFD will help solve this problem and improve the speed of fault detection.

PICOS implementation of BFD supports OSPF, BGP, and PIM protocols.

Single-Hop and Multi-Hop BFD

You can create a single-hop or multi-hop BFD session on an IP link to detect faults quickly:

- **Single-hop BFD** is the IP connectivity detection of two directly connected systems, with only one hop.
- **Multi-hop BFD** detects IP connectivity of paths between two indirectly connected systems, which may span multiple hops.

BFD Working Process

The main working process of BFD is as follows:

1. BFD first establishes a BFD session on a link between two endpoints (established by relying on the upper-layer protocol, e.g., when OSPF neighbors are established, the neighbor information is synced to BFD to establish BFD neighbors based on this information).

2. After two systems establish a BFD session, they will periodically send BFD control packets along the path between them. If a link failure is detected, the BFD neighbor is removed and the upper-layer protocol is immediately notified to handle the path loss issue.

BFD Session Establishment

BFD session can be established in two ways: static establishment and dynamic establishment:

- **Static Establishment**

BFD session parameters, including the local address and peer address, are manually specified. The neighbor adjacency will be established after all the configurations are manually committed.

- **Dynamic Establishment**

BFD sessions are established based on the neighbor adjacencies established by other routing protocols such as OSPF, BGP, and PIM, we refer to this as Dynamic Establishment of BFD.

Echo Function

Once the BFD session is Up, a system can choose to start the Echo function. When the Echo function is active, a stream of BFD Echo packets is transmitted in such a way as to have the other system loop them back through its forwarding path. If a number of packets of the echoed data stream are not received, the session is declared to be down. For more details, please refer to RFC 5880.

This may reduce round-trip jitter and thus allow more aggressive Detection Times, as well as potentially detecting some classes of failure that might not otherwise be detected.

The Echo function can be run independently in each direction between a pair of systems.

When the Echo function is active, a system SHOULD set the minimum receive interval (the command is **set protocols bfd** [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer**<*peer-ip*> **receive-interval <***receive-interval***>**) to a value of not less than one second (1,000,000 microseconds). This is intended to keep received BFD Control traffic at a negligible level, since the actual detection function is being performed using BFD Echo packets.

Users can use the command **set protocols bfd** [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo-mode** to enable echo function.

NOTEs:
- Echo function is only supported in single-hop BFD case.
- BFD echo mode is incompatible with that on other vendors, that is, echo mode can work only between PICOS switches.

Configuring BFD

Users can configure static BFD or dynamic BFD (BFD for OSPF, BFD for BGP or BFD for PIM protocols). Please refer to the following sections for configuration.

- Configuring Static BFD
- Configuring Dynamic BFD

Configuring Static BFD

To statically establish a BFD session, users need to manually set the BFD session parameters, such as the local address and peer address. The neighbor adjacency will be established after all the configurations are manually committed.

The following two sections list the configuration steps and commands for how to establish a single-hop session and a multi-hop BFD session.

Configuring Single-Hop BFD

Step 1 Enable single-hop BFD.

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> [**local-address** <*local-ip*>]

Step 2 (Optional) Configure single-hop BFD session parameters.

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **receive-interval <***receive-interval***>**

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **transmit-interval <***transmit-interval***>**

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **detect-multiplier <***MULTIPLIER***>**

Step 3 (Optional) Enable BFD echo function.

> **NOTEs:**
> - Echo function is only supported in single-hop BFD case.
> - BFD echo mode is incompatible with that on other vendors, that is, echo mode can work only between PICOS switches.

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **echo-mode**

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **echo receive-interval** [**<***receive-interval***> | disabled**]

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] **peer** <*peer-ip*> **echo transmit-interval <***transmit-interval***>**

Step 4 Commit the configurations.

commit

Configuring Multi-Hop BFD

Step 1 Enable multi-hop BFD.

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer** <*peer-ip*> [**local-address** <*local-ip*>]

Step 2 (Optional) Configure multi-hop BFD session parameters.

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer** <*peer-ip*> **local-address** <*local-ip*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer** <*peer-ip*> **local-address** <*local-ip*> **receive-interval <***receive-interval***>**

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer** <*peer-ip*> **local-address** <*local-ip*> **transmit-interval <***transmit-interval***>**

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer** <*peer-ip*> **local-address** <*local-ip*> **detect-multiplier <***MULTIPLIER***>**

Step 3 **Commit the configurations.**

commit

Configuring Dynamic BFD

In Dynamic BFD sessions are established based on the neighbor adjacencies established by the routing protocols such as OSPF, BGP, and PIM.

Link failures or topology changes on the network can lead to route recalculation. It is important to shorten the convergence time of routing protocols to improve the availability of the network. Users can enable the association between BFD and the routing protocols to quickly detect faults on links between network devices and achieve fast route convergence.

The following sections list the configuration steps and commands for how to establish BFD sessions for OSPFv2, OSPFv3, BGP and PIM.

Note that echo function is only supported in the single-hop BFD case.

Configuring BFD for OSPFv2

Step 1 (Optional) Create a profile to modify BFD session parameters.

set protocols bfd profile <*profile-name*> **detect-multiplier <***MULTIPLIER***>**

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Step 2 (Optional) Create a profile to enable BFD echo function.

set protocols bfd profile <*profile-name*> **echo-mode**

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Step 3 Enable BFD for OSPFv2.

set protocols ospf interface <*vlan-interface*> **bfd** [**profile** <*profile-name*>]

Step 4 Commit the configurations.

commit

Configuring BFD for OSPFv3

Step 1 (Optional) Create a profile to modify BFD session parameters.

set protocols bfd profile <*profile-name*> **detect-multiplier <***MULTIPLIER***>**

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Step 2 (Optional) Create a profile to enable BFD echo function.

set protocols bfd profile <*profile-name*> **echo-mode**

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Step 3 Enable BFD for OSPFv3.

set protocols ospf6 interface <*vlan-interface*> **bfd** [**profile** <*profile-name*>]

Step 4 Commit the configurations.

commit

Configuring BFD for BGP

Step 1 (Optional) Create a profile to modify BFD session parameters.

set protocols bfd profile <*profile-name*> **detect-multiplier <***MULTIPLIER***>**

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Step 2 (Optional) Create a profile to enable BFD echo function.

set protocols bfd profile <*profile-name*> **echo-mode**

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Step 3 Enable BFD for BGP.

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** **bfd** [**profile** <*profile-name*>]

Step 4 Commit the configurations.

commit

Configuring BFD for PIM

Step 1 (Optional) Create a profile to modify BFD session parameters.

set protocols bfd profile <*profile-name*> **detect-multiplier <***MULTIPLIER***>**

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Step 2 (Optional) Create a profile to enable BFD echo function.

set protocols bfd profile <*profile-name*> **echo-mode**

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Step 3 Enable BFD for PIM.

set protocols pim interface <*vlan-interface*> **bfd** [**profile** <*profile-name*>]

Step 4 Commit the configurations.

commit

Configuration Examples of BFD

- Example for Configuring Single-Hop BFD
- Example for Configuring Multi-Hop BFD
- Example for Configuring BFD for BGP
- Example for Configuring BFD for OSPF
- Example for Configuring BFD for PIM-SM

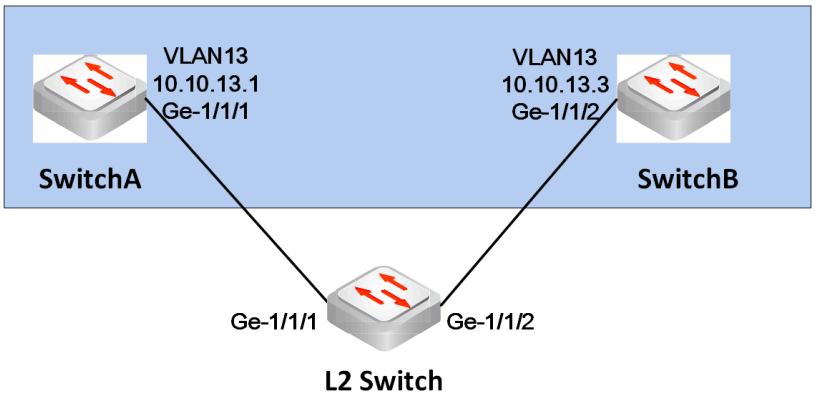
Example for Configuring Single-Hop BFD

- Networking Requirements
  - Figure 1 Single-hop BFD for detecting faults
- Procedure
  - Switch A
  - L2 Switch
  - Switch B
- Verify the Configuration

Networking Requirements

As shown in Figure 1, SwitchA and SwitchB are connected through the Layer 2 switch. Users can configure BFD sessions on SwitchA and SwitchB so that faults on the link between SwitchA and SwitchB can to be detected rapidly.

Figure 1 Single-hop BFD for detecting faults



Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 13
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@SwitchA# set l3-interface vlan-interface vlan13 address 10.10.13.1 prefix-length 24
admin@SwitchA# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Enable BFD and create a single-hop BFD session on SwitchA.

```
admin@SwitchA# set protocols bfd interface vlan13 peer 10.10.13.3
```

Step3 Commit the configurations.

```
admin@SwitchA# commit
```

L2 Switch

Step1 Configure the VLAN.

```
admin@L2Switch# set vlans vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
```

Step2 Commit the configurations.

```
admin@L2Switch# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 13
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@SwitchB# set l3-interface vlan-interface vlan13 address 10.10.13.3 prefix-length 24
admin@SwitchB# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Enable BFD and create a BFD session on SwitchB.

```
admin@SwitchB# set protocols bfd interface vlan13 peer 10.10.13.1
```

Step3 Commit the configurations.

```
admin@SwitchB# commit
```

Verify the Configuration

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a single-hop BFD session is set up and its status is up.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2107973506 10.10.13.1                            10.10.13.3                           up

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1620807635 10.10.13.3                            10.10.13.1                           up
```

- Run the **set interface gigabit-ethernet ge-1/1/2 disable true** command on the GE-1/1/2 interface of SwitchB to simulate a link fault.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 disable true
admin@SwitchB# commit
```

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a single-hop BFD session is set up and its status is down.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2107973506 10.10.13.1                            10.10.13.3                           down

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1620807635 10.10.13.3                            10.10.13.1                           down
```

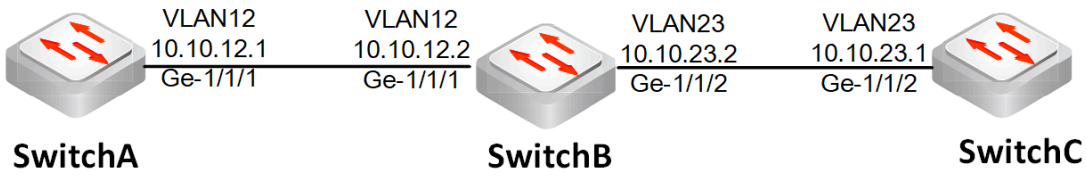
Example for Configuring Multi-Hop BFD

- Networking Requirements
  - Figure 1 Multi-hop BFD for detecting faults
- Procedure
  - Switch A
  - Switch B
  - Switch C
- Verify the Configuration

Networking Requirements

As shown in Figure 1, SwitchA and SwitchC are connected through the Layer 3 switch SwitchB. Users can configure multi-hop BFD session on SwitchA and SwitchC so that faults on the multi-hop link between SwitchA and SwitchC can be detected rapidly.

Figure 1 Multi-hop BFD for detecting faults



Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 12
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 12
admin@SwitchA# set l3-interface vlan-interface vlan12 address 10.10.12.1 prefix-length 24
admin@SwitchA# set vlans vlan-id 12 l3-interface vlan12
```

Step2 Configure a static route for connection between SwitchA and SwitchC.

```
admin@SwitchA# set protocols static route 10.10.23.0/24 next-hop 10.10.12.2
```

Step3 Enable BFD and create a multi-hop BFD session on SwitchA.

```
admin@SwitchA# set protocols bfd multihop peer 10.10.23.1 local-address 10.10.12.1
```

Step4 Commit the configurations.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 12
admin@SwitchB# set vlans vlan-id 23
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 12
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 23
admin@SwitchB# set l3-interface vlan-interface vlan12 address 10.10.12.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan23 address 10.10.23.2 prefix-length 24
admin@SwitchB# set vlans vlan-id 12 l3-interface vlan12
admin@SwitchB# set vlans vlan-id 23 l3-interface vlan23
```

Step2 Commit the configurations.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 23
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 23
admin@SwitchC# set l3-interface vlan-interface vlan23 address 10.10.23.1 prefix-length 24
admin@SwitchC# set vlans vlan-id 23 l3-interface vlan23
```

Step2 Configure a static route for connection between SwitchA and SwitchC.

```
admin@SwitchC# set protocols static route 10.10.12.0/24 next-hop 10.10.23.2
```

Step3 Enable BFD and create a multi-hop BFD session on SwitchC.

```
admin@SwitchC# set protocols bfd multihop peer 10.10.12.1 local-address 10.10.23.1
```

Step4 Commit the configurations.

```
admin@SwitchC# commit
```

Verify the Configuration

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchC. You can see that a multi-hop BFD session is set up and its status is up.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2486827319 10.10.12.1                            10.10.23.1                           up

admin@SwitchC# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1810426318 10.10.23.1                            10.10.12.1                           up
```

- Run the **set interface gigabit-ethernet ge-1/1/2 disable true** command on the GE-1/1/2 interface of SwitchB to simulate a link fault.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 disable true
admin@SwitchB# commit
```

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchC. You can see that a multi-hop BFD session is set up and its status is down.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2486827319 10.10.12.1                            10.10.23.1                           down

admin@SwitchC# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1810426318 10.10.23.1                            10.10.12.1                           down
```

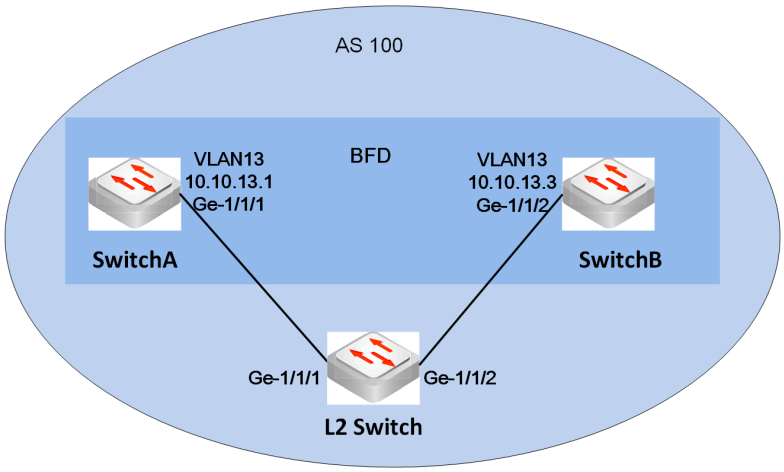
Example for Configuring BFD for BGP

- Networking Requirements
  - Figure 1 Configuring BFD for BGP
- Procedure
  - Switch A
  - L2 Switch
  - Switch B
- Verify the Configuration

Networking Requirements

As shown in Figure 1, BGP is established between SwitchA and SwitchB, and the L2 switch between SwitchA and SwitchB only provides the transparent transmission function. Users can configure BFD sessions on SwitchA and SwitchB so that faults on the link between SwitchA and SwitchB can be detected rapidly.

Figure 1 Configuring BFD for BGP



Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 13
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@SwitchA# set l3-interface vlan-interface vlan13 address 10.10.13.1 prefix-length 24
admin@SwitchA# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic BGP functions.

```
admin@SwitchA# set protocols bgp local-as 100
admin@SwitchA# set protocols bgp router-id 1.1.1.1
admin@SwitchA# set protocols bgp neighbor 10.10.13.3 remote-as 100
```

Step3 Enable BFD and create a BFD session for BGP on SwitchA.

```
admin@SwitchA# set protocols bgp neighbor 10.10.13.3 bfd
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

L2 Switch

Step1 Configure the VLAN.

```
admin@L2Switch# set vlans vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
```

Step2 Commit the configuration.

```
admin@L2Switch# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 13
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@SwitchB# set l3-interface vlan-interface vlan13 address 10.10.13.3 prefix-length 24
admin@SwitchB# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic BGP functions.

```
admin@SwitchB# set protocols bgp local-as 100
admin@SwitchB# set protocols bgp router-id 3.3.3.3
admin@SwitchB# set protocols bgp neighbor 10.10.13.1 remote-as 100
```

Step3 Enable BFD and create a BFD session for BGP on SwitchB.

```
admin@SwitchB# set protocols bgp neighbor 10.10.13.1 bfd
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Verify the Configuration

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up and its status is up.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2732266946 10.10.13.1                            10.10.13.3                           up

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
570407432 10.10.13.3                            10.10.13.1                           up
```

- Run the **set interface gigabit-ethernet ge-1/1/2 disable true** command on the GE-1/1/2 interface of SwitchB to simulate a link fault.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 disable true
admin@SwitchB# commit
```

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up but its status is down.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
2732266946 10.10.13.1                            10.10.13.3                           down

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
```

```
=========  ============                          ===========                          ======
570407432 10.10.13.3                             10.10.13.1                           down
```

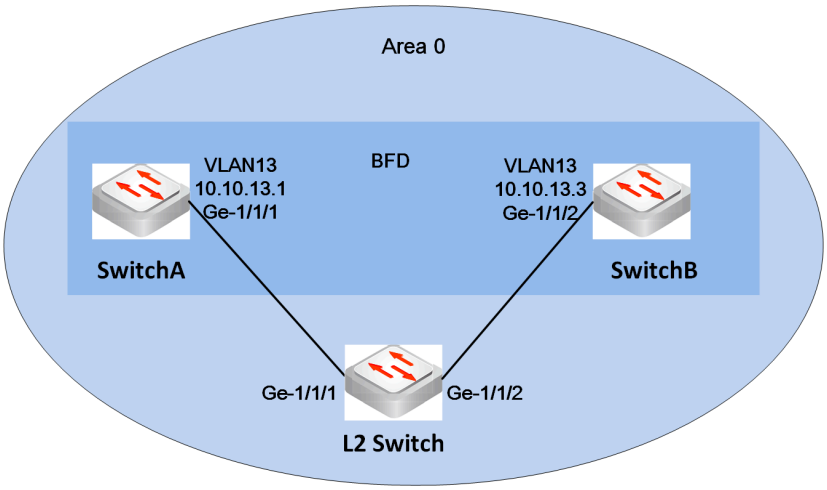
Example for Configuring BFD for OSPF

- Networking Requirements
  - Figure 1 Configuring BFD for OSPF
- Procedure
  - Switch A
  - L2 Switch
  - Switch B
- Verify the Configuration

Networking Requirements

As shown in Figure 1, OSPF is established between SwitchA and SwitchB, and the L2 switch between SwitchA and SwitchB only provides the transparent transmission function. Users can configure BFD sessions on SwitchA and SwitchB so that faults on the link between SwitchA and SwitchB can be detected rapidly.

Figure 1 Configuring BFD for OSPF



Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 13
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@SwitchA# set l3-interface vlan-interface vlan13 address 10.10.13.1 prefix-length 24
admin@SwitchA# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic OSPF functions.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf interface vlan13 area 0
```

Step3 Enable BFD and create a BFD session for OSPF on SwitchA.

```
admin@SwitchA# set protocols ospf interface vlan13 bfd
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

L2 Switch

Step1 Configure the VLAN.

```
admin@L2Switch# set vlans vlan-id 13
```

```
admin@L2Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
```

Step2 Commit the configuration.

```
admin@L2Switch# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 13
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@SwitchB# set l3-interface vlan-interface vlan13 address 10.10.13.3 prefix-length 24
admin@SwitchB# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic OSPF functions.

```
admin@SwitchB# set protocols ospf router-id 3.3.3.3
admin@SwitchB# set protocols ospf interface vlan13 area 0
```

Step3 Enable BFD and create a BFD session for OSPF on SwitchC.

```
admin@SwitchB# set protocols ospf interface vlan13 bfd
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Verify the Configuration

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up and its status is up.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1116990599 10.10.13.1                            10.10.13.3                           up

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1078838095 10.10.13.3                            10.10.13.1                           up
```

- Run the **set interface gigabit-ethernet ge-1/1/2 disable true** command on the GE-1/1/2 interface of SwitchB to simulate a link fault.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 disable true
admin@SwitchB# commit
```

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up but its status is down.

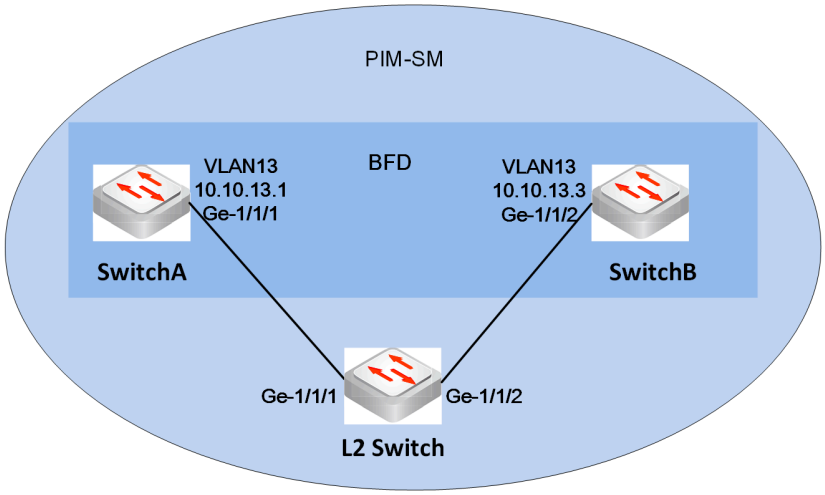
```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1116990599 10.10.13.1                            10.10.13.3                           down

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1078838095 10.10.13.3                            10.10.13.1                           down
```

Example for Configuring BFD for PIM-SM

Networking Requirements

As shown in Figure 1, PIM-SM is configured between SwitchA and SwitchB, and the L2 switch between SwitchA and SwitchB only provides the transparent transmission function. Users can configure BFD sessions on SwitchA and SwitchB so that faults on the link between SwitchA and SwitchB can be detected rapidly.

Figure 1 Configuring BFD for PIM-SM



Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 13
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@SwitchA# set l3-interface vlan-interface vlan13 address 10.10.13.1 prefix-length 24
admin@SwitchA# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic PIM functions.

```
admin@SwitchA# set protocols pim interface vlan13 sm
```

Step3 Enable BFD and create a BFD session for PIM on SwitchA.

```
admin@SwitchA# set protocols pim interface vlan13 bfd
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

L2 Switch

Step1 Configure the VLAN.

```
admin@L2Switch# set vlans vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 13
admin@L2Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
```

Step2 Commit the configuration.

```
admin@L2Switch# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 13
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@SwitchB# set l3-interface vlan-interface vlan13 address 10.10.13.3 prefix-length 24
admin@SwitchB# set vlans vlan-id 13 l3-interface vlan13
```

Step2 Configure basic PIM functions.

```
admin@SwitchB# set protocols pim interface vlan13 sm
```

Step3 Enable BFD and create a BFD session for PIM on SwitchB.

```
admin@SwitchB# set protocols pim interface vlan13 bfd
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Verify the Configuration

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up and its status is up.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
406990062  10.10.13.1                            10.10.13.3                           up

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1576079599 10.10.13.3                            10.10.13.1                           up
```

- Run command **run show pim neighbor** to show information about PIM neighbors.

```
admin@SwitchA# run show pim neighbor
Interface               Neighbor    Uptime  Holdtime  DR Pri
vlan13                10.10.13.3  00:01:42  00:01:33       1

admin@SwitchB# run show pim neighbor
Interface               Neighbor    Uptime  Holdtime  DR Pri
vlan13                10.10.13.1  00:02:51  00:01:24       1
```

- Run the **set interface gigabit-ethernet ge-1/1/2 disable true** command on the GE-1/1/2 interface of SwitchB to simulate a link fault.

```
admin@SwitchB# set interface gigabit-ethernet ge-1/1/2 disable true
admin@SwitchB# commit
```

- After the configuration is complete, run the command **run show bfd peers brief** on SwitchA and SwitchB. You can see that a BFD session between SwitchA and SwitchB is set up but its status is down.

```
admin@SwitchA# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
406990062  10.10.13.1                            10.10.13.3                           down

admin@SwitchB# run show bfd peers brief
Session count: 1
SessionId  LocalAddress                          PeerAddress                          Status
=========  ============                         ===========                          ======
1576079599 10.10.13.3                            10.10.13.1                           down
```

RFC Lists for BFD

The following table lists the RFC documents related to BFD function.

RFC	Description
RFC 5880	Bidirectional Forwarding Detection (BFD)
RFC 5881	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
RFC 5882	Generic Application of Bidirectional Forwarding Detection (BFD)
RFC 5883	Bidirectional Forwarding Detection (BFD) for Multihop Paths

RIP/RIPng Configuration

- RIP/RIPng Overview
- Enabling RIP/RIPng
- Configuring RIP Version
- Configuring RIP Route Redistribute
- Configuring RIPv2 Authentication
- Configuring RIP to Advertise Default Routes
- Example for Configuring Basic RIP
- Example for Configuring Basic RIPng
- RFC Lists for RIP/RIPng

RIP/RIPng Overview

RIP is short for Routing Information Protocol, which is a simple Interior Gateway Protocol. RIP exchanges routing information through UDP packets using the port number 520.

RIP is a protocol based on the Distance-Vector algorithm, which uses the Hop Count as the metric to measure the distance to the destination network. The metric is equal to the number of devices between the local network and the destination network, the number of hops from a device to a network directly connected to it is 0. To limit the convergence time, RIP specifies that the metric value is an integer between 0 and 15, anything greater than 15 is considered infinite, i.e., the destination network or host is unreachable. This limitation makes it impossible for RIP to be used in large networks.

RIP protocol is applied in IPv4 networks, while in IPv6 networks, the corresponding RIPng routing protocol is used. RIPng refers to RIP next generation protocol, mainly used to provide routing functionality in IPv6 networks, which is an important component of routing technology in IPv6 networks.

Enabling RIP/RIPng

- Enabling RIP/RIPng on a Specified Network Segment
- Enabling RIP/RIPng on an L3 Interface

RIP/RIPng runs only on interfaces on specified network segments. For interfaces that are not on the specified network segment, RIP/RIPng neither receives and sends routes on it, nor forwards its interface routes out. Users can enable RIP/RIPng in the following two ways:

- Enabling RIP/RIPng on a Specified Network Segment
- Enabling RIP/RIPng on an L3 Interface

Enabling RIP/RIPng on a Specified Network Segment

The following command enables RIP routing on the specified network segments 10.0.0.0/24 and 192.168.10.0/24.

```
admin@PICOS# set protocols rip network 10.0.0.0/24
admin@PICOS# set protocols rip network 192.168.10.0/24
admin@PICOS# commit
```

The following command enables RIPng routing on the specified network segments FC00:0:0:1000::0/64.

```
admin@PICOS# set protocols ripng network FC00:0:0:1000::0/64
admin@PICOS# commit
```

Enabling RIP/RIPng on an L3 Interface

Users can enable RIP/RIPng on an L3 interface, which can be a VLAN interface, routed interface or loopback interface. All routes for all network segments on this interface will be advertised via RIP/RIPng messages.

> **NOTE:**
> Although it is supported to enable RIP on a loopback interface by using command **set protocols rip interface** <*looplack-interface-name*>, but it doesn't work for RIPng by using command **set protocols ripng interface** <*looplack-interface-name*>. Users can use command **set protocols ripng route** <*loopback-IPv6-net*> command to set RIPng static network routing announcement for loopback interface.

The following command enables RIP routing to send and receive routes on all network segments on VLAN interface *vlan100*.

```
admin@PICOS# set protocols rip interface vlan100
admin@PICOS# commit
```

The following command enables RIPng routing to send and receive routes on all network segments on VLAN interface *vlan1000*.

```
admin@PICOS# set protocols ripng interface vlan1000
admin@PICOS# commit
```

Configuring RIP Version

The versions of RIP include RIPv1 and RIPv2, which have different functions. RIPv1 is a Classful Routing Protocol, which only supports protocol messages in broadcast mode. RIPv2 is a Classless Routing Protocol that supports sending update messages in multicast mode. RIPv1 does not support either route aggregation or Discontiguous Subnet. But RIPv2 supports both features. Users can configure the version number of RIP on the device running RIP protocol as needed.

Figure 1 and **Figure 2** show the packet format of RIPv1 and RIPv2.

Figure 1. RIPv1 Packet Format

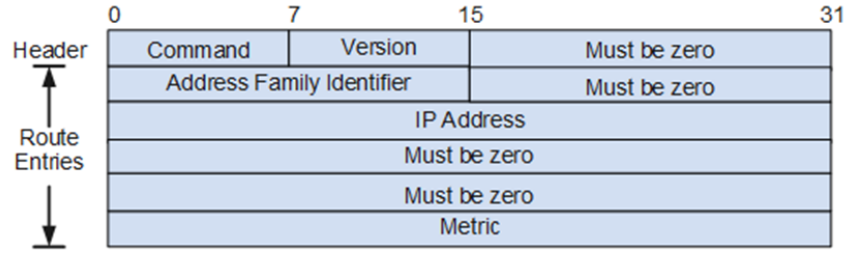
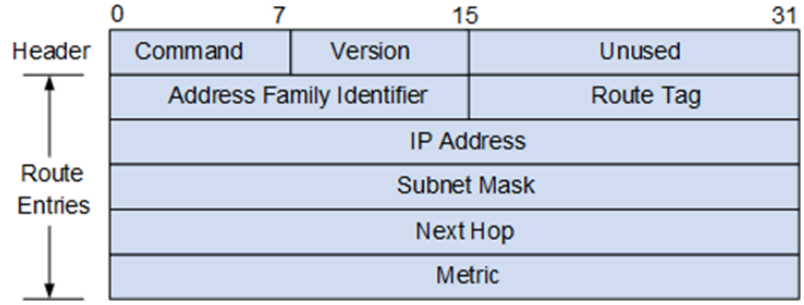


Figure 2. RIPv2 Packet Format



The **set protocols rip** [**vrf** <*vrf-name*>] **version** <**1**|**2**> command configures the RIP version to accept for receiving and sending RIP packets. RIP version can be either RIPv1 and RIPv2. By default, RIP version is RIPv2. The optional parameter **vrf** can be used to specify RIP for a particular VRF. If VRF is not defined then RIP takes effect for the default VRF.

This example configures RIP version to RIPv1.

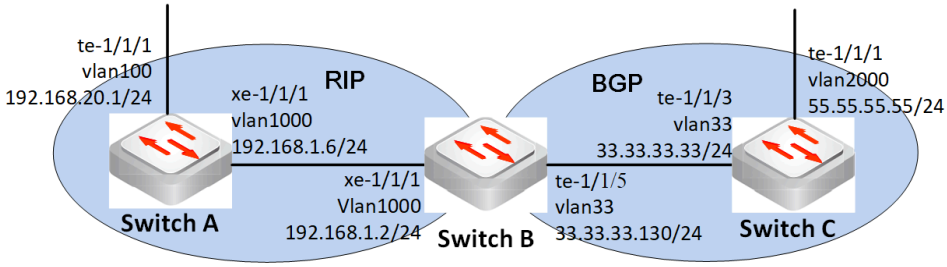
```
admin@PICOS# set protocols rip version 1
admin@PICOS# commit
```

Configuring RIP Route Redistribute

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - View RIP Route Table on Switch A
  - Configuring Switch B to Import Route between BGP and RIP
  - View RIP Route Table on Switch A

Networking Requirements

Figure 1. RIP Route Redistribute Example



As shown in **Figure 1**, there are three switches (Switch A, Switch B and Switch C) in this sample network. RIPv2 routing protocol runs between Switch A and Switch B, and BGP routing protocol runs between Switch B and Switch C. To enable communication between Switch A and Switch C, you need to configure to redistribute RIP routes to BGP routes, and BGP routes to RIP routes on Switch B.

Follow the configuration roadmap below to complete the configuration:

1. Configure VLAN interface and IP address for each interface to make the network reachable.
2. Enable RIP on Switch A and Switch B, and enable BGP on Switch B and Switch C.
3. On Switch B, configure route redistribution between route protocol RIP and BGP.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchA# set vlans vlan-id 1000 l3-interface vlan1000
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 100
admin@SwitchA# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching vlan members 1000
admin@SwitchA# set l3-interface vlan-interface vlan100 address 192.168.20.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan1000 address 192.168.1.6 prefix-length 24
```

Step2 Enable RIP for the network segment.

```
admin@SwitchA# set protocols rip network 192.168.20.0/24
admin@SwitchA# set protocols rip network 192.168.1.0/24
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 1000 l3-interface vlan1000
admin@SwitchB# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchB# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching vlan members 1000
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching vlan members 33
admin@SwitchB# set l3-interface vlan-interface vlan1000 address 192.168.1.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan33 address 33.33.33.130 prefix-length 24
```

Step2 Enable RIP for the specified network segment.

```
admin@SwitchB# set protocols rip network 192.168.1.0/24
admin@SwitchB# set protocols rip network 33.33.33.0/24
```

Step3 Configure EBGP connection between Switch B and Switch C.

```
admin@SwitchB# set protocols bgp local-as 20000
admin@SwitchB# set protocols bgp router-id 2.2.2.2
admin@SwitchB# set protocols bgp ebgp-requires-policy false
admin@SwitchB# set protocols bgp ipv4-unicast network 192.168.1.0/24
admin@SwitchB# set protocols bgp neighbor 33.33.33.33 remote-as 30000
```

Step4 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step5 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchC# set vlans vlan-id 2000 l3-interface vlan2000
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 33
admin@SwitchC# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 2000
admin@SwitchC# set l3-interface vlan-interface vlan33 address 33.33.33.33 prefix-length 24
admin@SwitchC# set l3-interface vlan-interface vlan2000 address 55.55.55.55 prefix-length 24
```

Step2 Configure EBGP connection between Switch B and Switch C.

```
admin@SwitchC# set protocols bgp local-as 30000
admin@SwitchC# set protocols bgp router-id 3.3.3.3
admin@SwitchC# set protocols bgp ebgp-requires-policy false
admin@SwitchC# set protocols bgp ipv4-unicast network 55.55.55.0/24
admin@SwitchC# set protocols bgp neighbor 33.33.33.130 remote-as 20000
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchC# commit
```

View RIP Route Table on Switch A

- On Switch A, use command **run show rip** to view RIP route table, 55.55.55.0/24 route is not existed.

```
admin@SwitchA# run show rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface
```

```
     Network            Next Hop         Metric From            Tag Time
R(n) 33.33.33.0/24      192.168.1.2           2 192.168.1.2       0 02:43
C(i) 192.168.1.0/24     0.0.0.0               1 self              0
C(i) 192.168.20.0/24    0.0.0.0               1 self              0
```

Configuring Switch B to Import Route between BGP and RIP

```
admin@SwitchB# set protocols rip redistribute bgp
admin@SwitchB# set protocols bgp ipv4-unicast redistribute rip
admin@SwitchB# commit
```

View RIP Route Table on Switch A

- On Switch A, use command **run show rip** to view RIP route table again, route 55.55.55.0/24 has been inserted to Switch A's routing table with metric value 2. Switch A and Switch C can communicate with each other now.

```
admin@SwitchA# run show rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 33.33.33.0/24      192.168.1.2           2 192.168.1.2       0 02:43
R(n) 55.55.55.0/24      192.168.1.2           2 192.168.1.2       0 02:43
C(i) 192.168.1.0/24     0.0.0.0               1 self              0
C(i) 192.168.20.0/24    0.0.0.0               1 self              0
```

Configuring RIPv2 Authentication

- Background
- Procedure
- Example

Background

RIPv2 allows packets to be authenticated via either an insecure plain text password, included with the packet, or via a more secure MD5 based HMAC (keyed-Hashing for Message AuthentiCation), RIPv1 can not be authenticated at all, thus when authentication is configured ripd will discard routing updates received via RIPv1 packets.

The MD5 Message-Digest Algorithm takes a message of arbitrary length as input and generates a 128 bit "fingerprint" or "message digest" as output. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.

When authentication is enabled, PICOS will ignore updates from unauthenticated peers, including RIPv1 peers. Although updates from unauthenticated peers are ignored, but requests for routes from unauthenticated peers are still honored.

Procedure

NOTEs:

- Both the **authentication mode** and **authentication string** need to be configured, and the value should be identical at both ends of the link.
- When configuring the authentication mode of RIP-2 messages, if *text* mode is used, the password will be saved in plaintext in the configuration file, which is a security risk. It is recommended to use *md5* mode to encrypt the password and save it.

Step 1 Choose one of the following authentication modes to configure:

- **MD5:**

set l3-interface vlan-interface <*vlan-interface*> **ip-rip authentication mode md5 auth-length** [**old-ripd** | **rfc**]

- **text:**

set l3-interface vlan-interface <*vlan-interface*> **ip-rip authentication mode text**

Step 2 Configure authentication string.

set l3-interface vlan-interface <*vlan-interface*> **ip-rip authentication string** <*string*>

Step 3 Commit the configuration.

commit

Example

The following example commands configure RIPv2 authentication mode to MD5 and the authentication string is *PICOS*.

```
admin@PICOS# set l3-interface vlan-interface vlan100 ip-rip authentication mode md5 auth-length rfc
admin@PICOS# set l3-interface vlan-interface vlan100 ip-rip authentication string PICOS
admin@PICOS# commit
```

Configuring RIP to Advertise Default Routes

In the routing table, the default route is a route to network 0.0.0.0 (also with a mask of 0.0.0.0). When the destination address of a message cannot match with any destination address in the routing table, the device will select the default route to forward the message.

The **set protocols rip** [**vrf** <*vrf-name*>] **default-information originate** command can be used to configure the current device to generate a default route to advertise to its neighbors. The optional parameter **vrf** can be used to specify RIP for a particular VRF. If VRF is not defined then RIP takes effect for the default VRF.

The following example configures the current device to generate a default route to advertise to its neighbors.

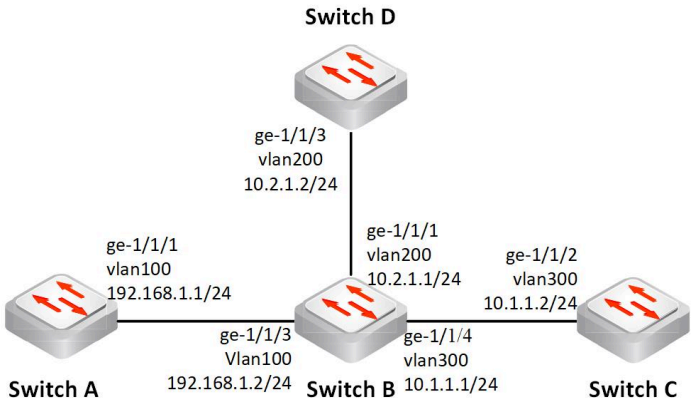
```
admin@PICOS# set protocols rip default-information originate
admin@PICOS# commit
```

Example for Configuring Basic RIP

- Networking Requirements
  - Figure 1. RIP Configuration Example
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
- Verifying the Configuration

Networking Requirements

Figure 1. RIP Configuration Example



As shown in **Figure 1**, there are four switches in a small network that require network interconnection on SwitchA, SwitchB, SwitchC, and SwitchD. Since it is a small network, it is recommended to configure RIPv2 routing protocol to achieve network interconnection of devices.

Follow the configuration roadmap below to complete the configuration:

1. Configure VLAN interface and IP address of each interface to make the network reachable.
2. Enable RIP on each switch to achieve basic network interconnection.
3. Run command **run show rip** to view RIP route information, **run show rip status** to view RIP general configuration information.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchA# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 100
admin@SwitchA# set l3-interface vlan-interface vlan100 address 192.168.1.1 prefix-length 24
```

Step2 Enable RIP for the specified network segment.

```
admin@SwitchA# set protocols rip network 192.168.1.0/24
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchB# set vlans vlan-id 200 l3-interface vlan200
admin@SwitchB# set vlans vlan-id 300 l3-interface vlan300
admin@SwitchB# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 200
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 100
admin@SwitchB# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching vlan members 300
admin@SwitchB# set l3-interface vlan-interface vlan100 address 192.168.1.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan200 address 10.2.1.1 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan300 address 10.1.1.1 prefix-length 24
```

Step2 Enable RIP for the specified network segment.

```
admin@SwitchB# set protocols rip network 192.168.1.0/24
admin@SwitchB# set protocols rip network 10.2.1.0/24
admin@SwitchB# set protocols rip network 10.1.1.0/24
```

Step3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 300 l3-interface vlan300
admin@SwitchC# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 300
admin@SwitchC# set l3-interface vlan-interface vlan300 address 10.1.1.2 prefix-length 24
```

Step2 Enable RIP for the specified network segment.

```
admin@SwitchC# set protocols rip network 10.1.1.0/24
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchC# commit
```

Switch D

Step1 Configure VLAN interface.

```
admin@SwitchD# set vlans vlan-id 200 l3-interface vlan200
admin@SwitchD# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 200
admin@SwitchD# set l3-interface vlan-interface vlan200 address 10.2.1.2 prefix-length 24
```

Step2 Enable RIP for the specified network segment.

```
admin@SwitchD# set protocols rip network 10.2.1.0/24
```

Step3 Enable IP routing.

```
admin@SwitchD# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchD# commit
```

Verifying the Configuration

- On Switch A, use command **run show rip** to view RIP route table.

```
admin@SwitchA# run show rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 10.2.1.0/24        192.168.1.2           2 192.168.1.2       0 15:22
R(n) 10.1.1.0/24        192.168.1.2           2 192.168.1.2       0 15:22
C(i) 192.168.1.0/24     0.0.0.0               1 self              0
```

- On Switch A, use command **run show rip status** to view RIP general configuration information.

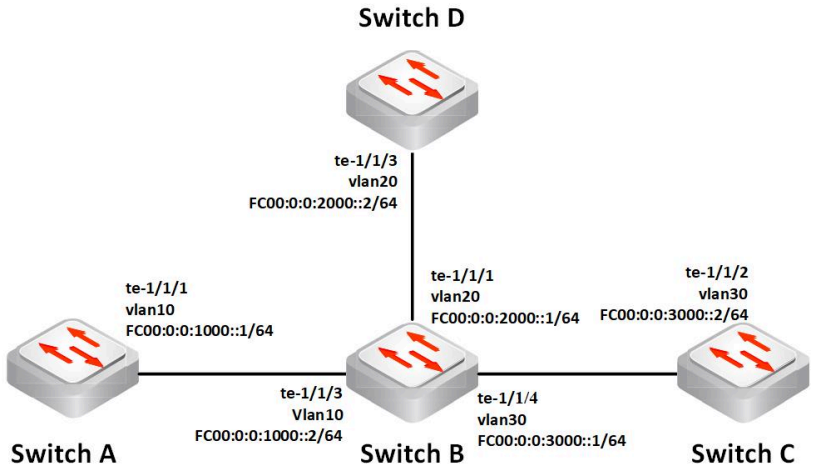
```
admin@SwitchA# run show rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 10 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive any version
    Interface        Send  Recv   Key-chain
    vlan100          2     1      2
  Routing for Networks:
    192.168.1.0/24
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
    192.168.1.2              0         0       120   00:00:20
  Distance: (default is 120)
```

Example for Configuring Basic RIPng

- Networking Requirements
  - Figure 1. RIPng Configuration Example
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Switch D
- Verifying the Configuration

Networking Requirements

Figure 1. RIPng Configuration Example



As shown in **Figure 1**, there are four switches in a small network. It is required to enable RIPng on all interfaces of SwitchA, SwitchB, SwitchC, and SwitchD to interconnect the network through RIPng.

Follow the configuration roadmap below to complete the configuration:

1. Configure the VLAN and IP address of each interface to make the network reachable.
2. Enable RIPng on each switch to basically achieve network interconnection.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 100
admin@SwitchA# set l3-interface vlan-interface vlan10 address FC00:0:0:1000::1 prefix-length 64
```

Step2 Enable RIPng for the specified network segment.

```
admin@SwitchA# set protocols ripng network FC00:0:0:1000::0/64
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 10 l3-interface vlan10
admin@SwitchB# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchB# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 20
admin@SwitchB# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 10
admin@SwitchB# set interface gigabit-ethernet te-1/1/4 family ethernet-switching vlan members 30
admin@SwitchB# set l3-interface vlan-interface vlan10 address FC00:0:0:1000::2 prefix-length 64
admin@SwitchB# set l3-interface vlan-interface vlan20 address FC00:0:0:2000::1 prefix-length 64
admin@SwitchB# set l3-interface vlan-interface vlan30 address FC00:0:0:3000::1 prefix-length 64
```

Step2 Enable RIPng for the specified network segment.

```
admin@SwitchB# set protocols ripng network FC00:0:0:1000::0/64
admin@SwitchB# set protocols ripng network FC00:0:0:2000::0/64
admin@SwitchB# set protocols ripng network FC00:0:0:3000::0/64
```

Step3 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 30 l3-interface vlan30
admin@SwitchC# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 30
admin@SwitchC# set l3-interface vlan-interface vlan30 address FC00:0:0:3000::2 prefix-length 64
```

Step2 Enable RIPng for the specified network segment.

```
admin@SwitchC# set protocols ripng network FC00:0:0:3000::0/64
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchC# commit
```

Switch D

Step1 Configure VLAN interface.

```
admin@SwitchD# set vlans vlan-id 20 l3-interface vlan20
admin@SwitchD# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 20
admin@SwitchD# set l3-interface vlan-interface vlan20 address FC00:0:0:2000::2 prefix-length 64
```

Step2 Enable RIPng for the specified network segment.

```
admin@SwitchD# set protocols ripng network FC00:0:0:3000::0/64
```

Step3 Enable IP routing.

```
admin@SwitchD# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchD# commit
```

Verifying the Configuration

- On Switch A, use command **run show ripng** to view RIPng route table.

```
admin@SwitchA# run show ripng
Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface, (a/S) - aggregated/Suppressed

   Network                    Next Hop                  Via       Metric Tag Time
C(i) FC00:0:0:1000::0/64
                              ::                        self       1      0
R(n) FC00:0:0:3000::0/64
                              FC00:0:0:1000::2          vlan10     2      0  02:58
R(n) FC00:0:0:2000::0/64
                              FC00:0:0:1000::2          vlan10     2      0  02:58
```

RFC Lists for RIP/RIPng

The following table lists the RFC documents related to RIP/RIPng function.

RFC	Description
RFC 1058	Routing Information Protocol. This document describes RIP protocol, describes the elements, characteristic, limitation of RIP version 1.
RFC 2453	RIP Version 2. This document specifies an extension of the Routing Information Protocol (RIP), to expand the amount of useful information carried in RIP messages and to add a measure of security.
RFC 2080	RIPng for IPv6. This document specifies a routing protocol for an IPv6 internet. It is based on protocols and algorithms currently in wide use in the IPv4 Internet.

Policy-Based Routing (PBR)

- Overview of PBR
- Configuring Policy-Based Routing
- Example for Configuring Policy-Based Routing

Overview of PBR

Policy-Based Routing (PBR) is a networking technique used to change the next hop IP address for traffic matching certain predefined policies or rule, rather than relying solely on traditional routing protocols and routing table entries. With PBR, administrators can direct traffic along specific paths according to various factors such as source/destination IP address, source/destination port.

After the device configures PBR, if the received messages match the rules of the PBR, they are forwarded according to the PBR route; if they fail to match, they are forwarded according to the destination address according to the traditional forwarding process.

The implementation and deployment of Policy-Based Routing consists of the following aspects:

1. **Policy Definition**: Administrators define policies that specify conditions under which certain types of traffic should be routed differently from the default routing behavior. A complete policy should be configured including **Match Rule**, **Action** and **Applying Interface**.

2. **Match Rule**: Policies in PBR include match rule, which are conditions that incoming packets must meet in order to be subjected to the policy. Match rule includes attributes such as source/destination IP address, source/destination port.

and is the logical operator between the matching fields with the same sequence number, that is, to be considered to match a PBR rule, the packets must match all the matching fields with the same sequence number.

3. **Action**: Once a packet matches the specified rule in a policy, an action is taken based on the policy configuration. This action involves routing the packet through a specific next-hop router/next-hop group routers or changing Quality of Service (QoS) policies such as DSCP value.

4. **Applying Interface**: Applying this policy to the VLAN interface where the traffic is coming in.

PBR provides flexibility and granular control over network traffic routing, allowing administrators to tailor routing decisions based on specific requirements or business needs, enhancing network performance, security, and flexibility.

Configuring Policy-Based Routing

Configuration Notes and Constraints
Configuring Policy-Based Routing
Procedure

Configuration Notes and Constraints

When configuring PBR, consider the following points:

- PBR processes only IP packets, L2 messages are not processed.
- PBR processes only unicast packets, multicast packets are not processed.
- PBR only handles forwarded packets, but does not handle locally originated packets (including local protocol and data packets).
- PBR policy applies to the VLAN interface where the traffic is coming in.
- Each PBR map can be applied to multiple Layer 3 interfaces, but each Layer 3 interface can have at most one PBR map configured.
- You cannot configure both IPv4 and IPv6 match conditions for the same PBR policy sequence.
- At least one match condition SHOULD be configured for a PBR policy.
- A PBR policy must contain an action configuration. However, if the action is configured with only DSCP, but no next-hop IP address, as shown in the following command line, this PBR policy only changes the DSCP value of the matched messages which will be forwarded based on the destination address according to the route table.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 10 match destination-ipv4 1.1.1.0/24
admin@PICOS# set routing pbr map PBR_map1 sequence 10 action dscp 40
```

- The next-hop address must be directly connected and reachable without supporting recursion.
- The next-hop address in the action configuration does not support the tunnel IP address.
- If a message matches the Discard rule in the firewall filter ACL and also matches the PBR rule, the Discard rule in the firewall filter ACL has a higher priority than the PBR rule, then the message will be discarded.
- IPSG ACL takes precedence over PBR ACL. If a packet is discarded by the IPSG module, it will have no chance to be processed by the PBR module.

Configuring Policy-Based Routing

Follow the configuration roadmap below to complete the deployment of Policy-Based Routing:

1. Configure PBR match rule.

Policies in PBR include match rule, which are conditions that incoming packets must meet in order to be subjected to the policy. Match rules include attributes such as source/destination IP address, source/destination port.

2. Configure PBR action.

Once a packet matches the specified rule in a policy, an action is taken based on the policy configuration. This action could involve routing the packet through a specific next-hop router/next-hop group routers, changing Quality of Service (QoS) policies such as DSCP value.

3. Configure applying interface for the PBR policy.

Applying this policy to the VLAN interface where the traffic is coming in.

Procedure

Step 1 Enable IP routing for L3 forwarding.

set ip routing enable true

Step 2 Configure the match rule for PBR traffic classification.

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-ipv4** <*ipv4-address*/prefix-length>

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv4** <*ipv4-address/prefix-length*>

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-port** <*destination-port*>

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-port** <*source-port*>

set routing pbr map <map-name> **sequence** <sequence-number> **match destination-ipv6** <ipv6-address/prefix-length>

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv6** <*ipv6-address/prefix-length*>

Step 3 Configure an action to redirect packets to a next-hop IPv4/IPv6 address for policy-based routing.

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action nexthop** <*ip-address*> [**nexthop-vrf** <*vrf-name*>]

Step 4 (Optional) Configure an action to redirect packets to a next-hop group IPv4/IPv6 addresses for policy-based routing.

set routing nexthop-group <*group-name*> **nexthop-vrf** <*vrf-name*> **nexthop** <*ip-address*>

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action nexthop-group** <*group-name*>

Step 5 Configure an action to modify the DSCP value in packets for policy-based routing.

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action dscp** <*dscp-value*>

Step 6 Apply the PBR policy to the VLAN interface where the traffic is coming in.

set routing pbr map <*map-name*> **vlan-interface** <*vlan-interface*>

Step 7 Commit the configuration.

commit

Step 8 View the configuration information of policy-based routing.

run show pbr map [<*map-name*>]

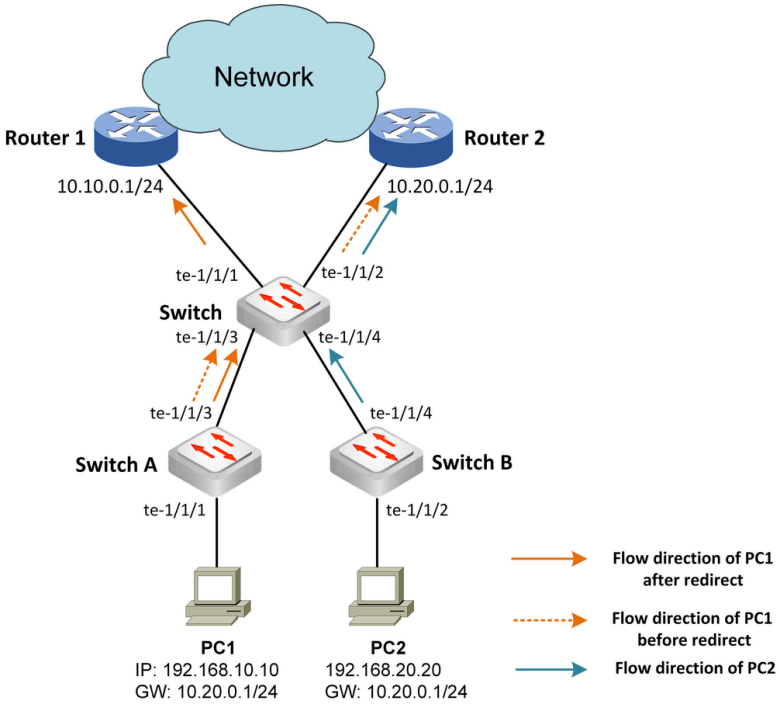
Example for Configuring Policy-Based Routing

Networking Requirements

Procedure on Switch

Networking Requirements

Figure 1. Policy-Based Routing Configuration Example



As shown in **Figure 1**, in the data center network, tenants PC1 and PC2 dually access to external network devices through the device Switch. The VLAN ID for PC1 is 100, and the IP address is 192.168.10.10. The VLAN ID for PC2 is 200, and the IP address is 192.168.20.20. The messages from both tenants are connected to external network devices through gateway Router 2 (10.20.0.1/24).

Now it is necessary to forward the packets from PC1 to external network devices through gateway Router 1 (10.10.0.1/24), and achieve routing redirection through policy-based routing to improve the tenant experience. The configuration parameters are shown in the table below.

Device	Port Name	VLAN Interface	IP Address
Switch	Te-1/1/1	VLAN100	10.10.0.2/24
Switch	Te-1/1/2	VLAN200	10.20.0.2/24
Switch	Te-1/1/3	VLAN300	192.168.10.2/24
Switch	Te-1/1/4	VLAN400	192.168.20.2/24

Follow the configuration roadmap below to complete the deployment of policy-based routing:

- Configure VLAN, VLAN interface and IP address on each switch to achieve network reachable. The configuration on the device Switch is provided in the following steps. Other devices have similar configurations and will therefore be ignored.
- On Switch, configure match rule based on the source IPv4 address 192.168.10.10/24 (IP address of PC1) for PBR traffic classification.

- On Switch, configure an action to redirect packets to a next-hop IP address 10.10.0.1/24 (IP address of Router 1) for policy-based routing.
- On Switch, apply the PBR policy to the VLAN interface VLAN300 where the traffic from PC1 is coming in.

Procedure on Switch

Step 1 Configure VLANs and VLAN interfaces.

```
admin@Switch# set vlans vlan-id 100
admin@Switch# set vlans vlan-id 200
admin@Switch# set vlans vlan-id 300
admin@Switch# set vlans vlan-id 400
admin@Switch# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@Switch# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 200
admin@Switch# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 300
admin@Switch# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 400
admin@Switch# set vlans vlan-id 100 l3-interface vlan100
admin@Switch# set vlans vlan-id 200 l3-interface vlan200
admin@Switch# set vlans vlan-id 300 l3-interface vlan300
admin@Switch# set vlans vlan-id 400 l3-interface vlan400
admin@Switch# set l3-interface vlan-interface vlan100 address 10.10.0.2 prefix-length 24
admin@Switch# set l3-interface vlan-interface vlan200 address 10.20.0.2 prefix-length 24
admin@Switch# set l3-interface vlan-interface vlan300 address 192.168.10.2 prefix-length 24
admin@Switch# set l3-interface vlan-interface vlan400 address 192.168.20.2 prefix-length 24
```

Step 2 Enable IP routing for L3 forwarding.

```
admin@Switch# set ip routing enable true
```

Step 3 Configure match rule based on the source IPv4 address 192.168.10.10/32 (IP address of PC1) for PBR traffic classification.

```
admin@Switch# set routing pbr map PBR_map1 sequence 100 match source-ipv4 192.168.10.10/32
```

Step 4 Configure an action to redirect packets to a next-hop IP address 10.10.0.1 (IP address of Router 1) for PBR.

```
admin@Switch# set routing pbr map PBR_map1 sequence 100 action nexthop 10.10.0.1
```

Step 5 Apply this policy PBR_map1 to the VLAN interface VLAN300 where the traffic from PC1 is coming in.

```
admin@Switch# set routing pbr map PBR_map1 vlan-interface vlan300
```

Step 6 Commit the configurations.

```
admin@Switch# commit
```

Step 7 View the configuration information of policy-based routing.

```
admin@Switch# run show pbr map PBR_map1
Sequence: 100
    match-condition:
        source-ipv4      192.168.10.10/32
action:
        nexthop     10.10.0.1 nexthop-vrf:
statistics:
        vlan300: 1864 pkts
```

IPv4 Source Guard (IPSG for IPv4)

- Overview
- Configuration Notes and Constraints
- Configuring IP Source Guard
  - Configure Static IP Source Guard Binding Entry
  - Configure Dynamic IP Source Guard Binding Entry
- Configuration Example
  - Networking Requirements
  - Procedure

Overview

IP Source Guard (IPSG) is a security feature implemented in network switches to mitigate IP address spoofing attacks. It generally works by ensuring that incoming packets on a network interface have a source IP address that matches an entry in the IP source guard binding table. Traffic from other IP addresses is dropped.

IP source guard binding table contains two types of entries: static entries and dynamic entries.

- **Static entries**: IP addresses that have been manually associated with a MAC address.
- **Dynamic entries**: IP addresses added through DHCP snooping binding table.

Dynamic table entry aging does not affect static table entries; that is to say, static table entries do not age.

IP source guard filtering items include either IP or IP+MAC based on specific interface and VLAN.

IP source guard permits traffic from the following sources, in addition to packets that match the entries in the IP source guard binding table:

- When DHCP snooping is enabled, IP source guard allows the reception of DHCP packets.
- IPv6 packets are not subjected to IP Source Guard checks.

By default, IP source guard is disabled. It must be enabled on each port where guarding is required.

Configuration Notes and Constraints

When configuring IP source guard, consider the following points:

- IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
- The interface that enables IPSG cannot be a DHCP snooping trust interface.
- IPSG has a higher priority than PBR (Policy-Based Routing) and 802.1X (downloadable ACL and dynamic ACL). When IPSG is enabled on the ingress interface and VLAN to which a packet belongs, the packet is subject to IPSG verification. As a result, it bypasses both PBR and 802.1X ACL matching processes.
- If a packet that matches the IP source guard entry also matches an ACL rule (such as a firewall filter ACL), and the action of the ACL rule is discard, then the packet will be discarded by the ACL regardless of other configurations.
- After configuring the IP source guard binding entry, it needs to be deployed to the hardware by the system. Therefore, the number of IP source guard binding entries supported by the switch depends on the current utilization of hardware resources. Of course, different switch platforms have different hardware performance, and thus support varying numbers of table entries.
- IPSG is not supported in MLAG scenarios.

Configuring IP Source Guard

Configuring IP Source Guard involves the following steps:

1. Configure IP Source Guard binding table entries in the following two ways:

- Static entries: Manually associate IP addresses with a MAC address.
- Enable DHCP snooping function to generate dynamic IP Source Guard entries. Dynamic entries are added through the DHCP Snooping binding table.

2. Enable IP source guard for a specific interface and VLAN.

> **NOTE**:
>
> - The command **set ip-source-guard interface** <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**> is used for step 2.
> - The interface and VLAN configured in step 2 should be consistent with the values in the IP source guard binding table.
> - When IP source guard is enabled on a specific interface and VLAN, all IP packets from this interface and VLAN will be dropped except that match the entries in the IP source guard binding table.
> - Packets received from other interfaces or VLANs that do not have IP source guard enabled will not be inspected by the IP source guard module and will be processed normally.

3. (Optional) Configure IP source guard filtering item for a specific interface and VLAN.
4. Verify the IP source guard entries.

You can enable both static and dynamic entries for IP source guard, or you can choose to enable only one of them. For users with dynamically assigned IP addresses, enabling DHCP Snooping is necessary.

Configure Static IP Source Guard Binding Entry

Step 1 Configure static IP source guard entries.

set ip-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

Step 2 Enable IP source guard based on specific interface and VLAN. Here, the interface and VLAN ID should be consistent with the values configured in the static IP source guard entries.

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true** | **false**>

Step 3 (Optional) Configure IP source guard filtering item based on specific interface and VLAN.

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify** <**ip** | **ip+mac**>

Step 4 Commit the configuration.

commit

Step 5 View the IP source guard binding entries.

run show ip-source-guard binding [**interface** <*interface-name*>]

Configure Dynamic IP Source Guard Binding Entry

Step 1 Enable DHCP snooping.

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

set protocols dhcp snooping trust-port <*interface-name*>

Step 2 Enable IP source guard based on specific interface and VLAN. Here, the interface and VLAN ID is the one that enables DHCP snooping.

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true** | **false**>

Step 3 (Optional) Configure IP source guard filtering item based on specific interface and VLAN. Here, the VLAN is the one that enables DHCP snooping.

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify** <**ip** | **ip+mac**>

Step 4 Commit the configuration.

commit

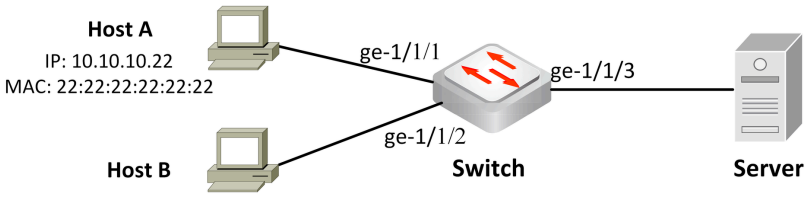
Step 5 View the IP source guard binding entries.

run show ip-source-guard binding [**interface** <*interface-name*>]

Configuration Example

Networking Requirements

Figure 1. IP Source Guard Configuration Example



As shown in **Figure 1**, on interfaces ge-1/1/1 and ge-1/1/2 of the device named Switch, enable IP Source Guard function to prevent IP address spoofing attacks. Enable both static IP source guard binding entry configuration and dynamic entry originating from the DHCP snooping binding table.

Follow the configuration roadmap below to complete the deployment on the Switch device:

1. Configure IP source guard binding table static entries for host A.
2. Enable DHCP Snooping for dynamically assigning IP to host B.
3. Enable IP source guard function for interfaces ge-1/1/1 and ge-1/1/2.
4. Configure IP source guard filtering item based on specific interface and VLAN.
5. Check the IP source guard entries.

Procedure

Step 1 Configure VLAN.

```
admin@PICOS# set vlans vlan-id 2
admin@PICOS# set vlans vlan-id 3
admin@PICOS# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@PICOS# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@PICOS#  set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 10,20
```

Step 2 Configure IP source guard static entry for host A.

```
admin@PICOS# set ip-source-guard binding ip 10.10.10.22 mac 3f:2c:99:51:48:01 interface ge-1/1/1 vlan 10
```

Step 3 For users with dynamically assigned IP addresses, DHCP snooping needs to be configured.

```
admin@PICOS# set protocols dhcp snooping vlan 20 disable false
admin@PICOS# set protocols dhcp snooping trust-port ge-1/1/3
```

Step 4 Enable IP source guard.

```
admin@PICOS# set ip-source-guard interface ge-1/1/1 vlan 10 enable true
admin@PICOS# set ip-source-guard interface ge-1/1/2 vlan 20 enable true
```

Step 5 Configure IP source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ip-source-guard interface ge-1/1/1 vlan 10 verify ip+mac
admin@PICOS# set ip-source-guard interface ge-1/1/2 vlan 20 verify ip+mac
```

Step 6 Commit the configuration.

```
admin@PICOS# commit
```

Step 7 View the IP source guard binding entries.

```
admin@PICOS# run show ip-source-guard binding
Total ipsg host count:     2
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------------
--------
22:22:22:22:22:22   10.10.10.22     ge-1/1/1        10        static           ip+mac              effective
54:9c:99:d3:09:5c   20.1.1.10       ge-1/1/2        20        dhcp-snooping    ip+mac              effective
```

IPv6 Source Guard (IPSG for IPv6)

- Overview
- Configuration Notes and Constraints
- Configuring IPv6 Source Guard
  - Configure Static IPv6 Source Guard Binding Entry
  - Configure Dynamic IPv6 Source Guard Binding Entry
- Configuration Example
  - Networking Requirements
  - Procedure

Overview

IPv6 Source Guard, or IPSG for IPv6, is a security feature implemented in network switches to mitigate IPv6 address spoofing attacks. It generally works by ensuring that incoming packets on a network interface have a source IPv6 address that matches an entry in the IPv6 source guard binding table. Traffic from other IPv6 addresses is dropped.

IPv6 source guard binding table contains two types of entries: static entries and dynamic entries.

- **Static entries**: IPv6 addresses that have been manually associated with a MAC address.
- **Dynamic entries**: IPv6 addresses added through DHCPv6 snooping binding table.

Dynamic table entry aging does not affect static table entries; that is to say, static table entries do not age.

IPv6 source guard filtering items include either IP or IP+MAC based on specific interface and VLAN.

IPv6 source guard permits traffic from the following sources, in addition to packets that match the entries in the IPv6 source guard binding table:

- When DHCPv6 snooping is enabled, IPv6 source guard allows the reception of DHCPv6 packets.
- IPv4 packets are not subjected to IPv6 Source Guard checks.

By default, IPv6 source guard is disabled. It must be enabled on each port where guarding is required.

Configuration Notes and Constraints

When configuring IPSG for IPv6, consider the following points:

- The entries of IPv6 subnet address without mask length in the IPv6 source guard binding table are ineffective for IPSG.
- IPSG for IPv6 be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
- The interface that enables IPSG for IPv6 cannot be a DHCPv6 snooping trust interface.
- IPSG for IPv6 has a higher priority than PBR (Policy-Based Routing) and 802.1X (downloadable ACL and dynamic ACL). When IPSG for IPv6 is enabled on the ingress interface and VLAN to which a packet belongs, the packet is subject to IPSG for IPv6 verification. As a result, it bypasses both PBR and 802.1X ACL matching processes.
- If a packet that matches the IPv6 source guard entry also matches an ACL rule (such as a firewall filter ACL), and the action of the ACL rule is discard, then the packet will be discarded by the ACL regardless of other configurations.
- After configuring the IPv6 source guard binding entry, it needs to be deployed to the hardware by the system. Therefore, the number of IPv6 source guard binding entries supported by the switch depends on the current utilization of hardware resources. Of course, different switch platforms have different hardware performance, and thus support varying numbers of table entries.
- IPSG for IPv6 is not supported in MLAG scenarios.

Configuring IPv6 Source Guard

Configuring IPv6 Source Guard involves the following steps:

1. Configure IPv6 Source Guard binding table entries in the following two ways:

- Static entries: Manually associate IPv6 addresses with a MAC address.
- Enable DHCPv6 snooping function to generate dynamic IPv6 Source Guard entries. Dynamic entries are added through the DHCPv6 Snooping binding table.

2. Enable IPv6 source guard for a specific interface and VLAN.

> **NOTE**:
>
> - The command **set ipv6-source-guard interface** <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**> is used for step 2.
> - The interface and VLAN configured in step 2 should be consistent with the values in the IPv6 source guard binding table.
> - When IPv6 source guard is enabled on a specific interface and VLAN, all IPv6 packets from this interface and VLAN will be dropped except that match the entries in the IPv6 source guard binding table.
> - Packets received from other interfaces or VLANs that do not have IPv6 source guard enabled will not be inspected by the IPv6 source guard module and will be processed normally.

3. (Optional) Configure IPv6 source guard filtering item for a specific interface and VLAN.
4. Verify the IPv6 source guard entries.

You can enable both static and dynamic entries for IPv6 source guard, or you can choose to enable only one of them. For users with dynamically assigned IPv6 addresses, enabling DHCPv6 Snooping is necessary.

Configure Static IPv6 Source Guard Binding Entry

Step 1 Configure static IPv6 source guard entries.

set ipv6-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

Step 2 Enable IPv6 source guard based on specific interface and VLAN. Here, the interface and VLAN ID should be consistent with the values configured in the static IPv6 source guard entries.

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true** | **false**>

Step 3 (Optional) Configure IPv6 source guard filtering item based on specific interface and VLAN.

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify** <**ip** | **ip+mac**>

Step 4 Commit the configuration.

commit

Step 5 View the IPv6 source guard binding entries.

run show ipv6-source-guard binding [**interface** <*interface-name*>]

Configure Dynamic IPv6 Source Guard Binding Entry

Step 1 Enable DHCPv6 snooping.

set protocols dhcpv6 snooping vlan <*vlan-id*> **disable** <**true** | **false**>

set protocols dhcpv6 snooping trust-port <*interface-name*>

Step 2 Enable IPv6 source guard based on specific interface and VLAN. Here, the interface and VLAN ID is the one that enables DHCPv6 snooping.

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true** | **false**>

Step 3 (Optional) Configure IPv6 source guard filtering item based on specific interface and VLAN. Here, the VLAN is the one that enables DHCPv6 snooping.

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify** <**ip** | **ip+mac**>

Step 4 Commit the configuration.

commit

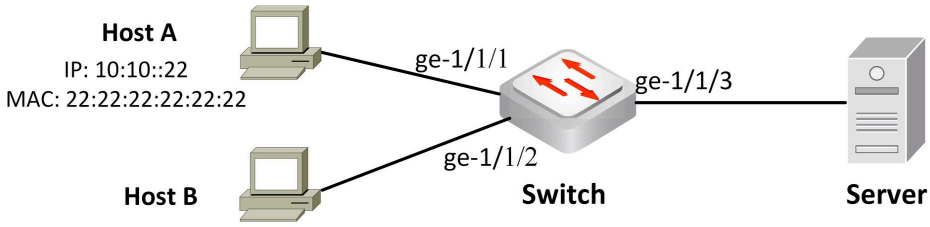
Step 5 View the IPv6 source guard binding entries.

run show ipv6-source-guard binding [**interface** <*interface-name*>]

Configuration Example

Networking Requirements

Figure 1. IPv6 Source Guard Configuration Example



As shown in **Figure 1**, on interfaces ge-1/1/1 and ge-1/1/2 of the device named Switch, enable IPv6 Source Guard function to prevent IPv6 address spoofing attacks. Enable both static IPv6 source guard binding entry configuration and dynamic entry originating from the DHCPv6 snooping binding table.

Follow the configuration roadmap below to complete the deployment on the Switch device:

1. Configure IPv6 source guard binding table static entries for host A.
2. Enable DHCPv6 Snooping for dynamically assigning IPv6 to host B.
3. Enable IPv6 source guard function for interfaces ge-1/1/1 and ge-1/1/2.
4. Configure IPv6 source guard filtering item based on specific interface and VLAN.
5. Check the IPv6 source guard entries.

Procedure

Step 1 Configure VLAN.

```
admin@PICOS# set vlans vlan-id 2
admin@PICOS# set vlans vlan-id 3
admin@PICOS# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 10
admin@PICOS# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 20
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@PICOS#  set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 10,20
```

Step 2 Configure IPv6 source guard static entry for host A.

```
admin@PICOS# set ipv6-source-guard binding ip 10:10::22 mac 22:22:22:22:22:22 interface ge-1/1/1 vlan 10
```

Step 3 For users with dynamically assigned IPv6 addresses, DHCPv6 snooping needs to be configured.

```
admin@PICOS# set protocols dhcpv6 snooping vlan 20 disable false
admin@PICOS# set protocols dhcpv6 snooping trust-port ge-1/1/3
```

Step 4 Enable IPv6 source guard.

```
admin@PICOS# set ipv6-source-guard interface ge-1/1/1 vlan 10 enable true
admin@PICOS# set ipv6-source-guard interface ge-1/1/2 vlan 20 enable true
```

Step 5 Configure IPv6 source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ipv6-source-guard interface ge-1/1/1 vlan 10 verify ip+mac
admin@PICOS# set ipv6-source-guard interface ge-1/1/2 vlan 20 verify ip+mac
```

Step 6 Commit the configuration.

```
admin@PICOS# commit
```

Step 7 View the IPv6 source guard binding entries.

```
admin@PICOS# run show ipv6-source-guard binding
Total ipsg6 host count:     2
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------------------
--------
22:22:22:22:22:22   10:10::22       ge-1/1/1        10        static             ip+mac              effective
54:9c:99:d3:09:5c   20::10          ge-1/1/2        20        dhcp6-snooping    ip+mac              effective
```

IPv6 RA Guard Configuration

> **NOTE:**
> Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.

When the switch receives an ingress router advertisement (RA) message, it will attempt to match the message via the RA guard. If the ingress port has the RA guard applied but is not a trusted port, the applied VLAN ID will be matched first. If the RA tag is matched with the VLAN ID, the RA guard will continue matching conditions to determine whether to forward or drop the RA message. If the RA tag is *not* matched with the VLAN ID, the applied interface will be matched (followed by the subsequent conditions). RA guard policy can be configured using hop-limit, managed-config-flag, other-config-flag, prefix, source-ipv6-addr, and source-mac-addr options.

RA guard function can be configured on physical interfaces, LAG ports, or in VLANs, and only checks the router advertisement (RA) packets on the untrusted ports with RA guard enabled. By default, all interfaces are untrusted with respect to RA guard. Trusted interfaces are manually specified.

- If RA guard is enabled on an untrusted interface, the RA message received on the interface will be checked by the RA guard policy. The RA packets only matched the RA guard policy can be processed and forwarded.
- If RA guard is disabled on an untrusted interface, the RA message received on the interface will not be checked by the RA guard policy. All the RA packets received on this interface are processed and forwarded without inspection.
- If RA guard is enabled on a trusted interface, the RA message received on the interface will not be checked by the RA guard policy. All the RA packets received on this interface are processed and forwarded without inspection.

Configuring RA Guard Policy

```
admin@XorPlus# set protocols neighbour ra-guard term guard1 from hop-limit 1
admin@XorPlus# set protocols neighbour ra-guard term guard1 from managed-config-flag false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols neighbour ra-guard term guard2 from prefix 2001:1:1:1::/64
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols neighbour ra-guard term guard3 from source-mac-addr 22:22:22:22:22:22
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Configuring Trusted-Port

No more than one RA guard can be applied to one interface. The RAs will be forwarded only if all conditions are matched. But if "trusted-port" has been configured for the RA guard, RAs will be forwarded on the trusted port regardless.

```
admin@XorPlus# set protocols neighbour ra-guard term 1 interface ge-1/1/1
admin@XorPlus# set protocols neighbour ra-guard term 1 interface ae1
admin@XorPlus# set protocols neighbour ra-guard term 1 vlan-id 2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#set protocols neighbour ra-guard trusted-port ge-1/1/2
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus# set protocols neighbour ra-guard term 2 vlan-id 3
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Displaying RA Guards

```
admin@XorPlus# run show ra-guard
Ra-guard: guard1
    cur hop limit  : 1..1
    managed configuration: Unset
    interface      : ae1
    vlan           : 2
    packet dropped : 0
    packet total   : 0

Ra-guard: guard2
    prefix         : 2001:1:1:1::/64
    vlan           : 3
    packet dropped : 0
```

```
    packet total   : 0

Ra-guard: guard3
    source mac address: 22:22:22:22:22:22
    packet dropped : 0
    packet total   : 0

trusted port: ge-1/1/2

admin@XorPlus# run show ra-guard name guard1
Ra-guard: guard1
    cur hop limit  : 1..1
    managed configuration: Unset
    interface      : ae1
    vlan           : 2
    packet dropped : 0
    packet total   : 0
```

IS-IS Configuration

- IS-IS Overview
- Configuring IS-IS Basic Function
- Configuring IS-IS Authentication
- Configuring LSP Packet Attributes
- Customizing Routes for IS-IS
- Configuring IS-IS Timers
- Controlling IS-IS Routing Information Exchange
- Adjusting SPF Calculation Time
- Configuration Examples of IS-IS

IS-IS Overview

- Overview
- Key features
- Application Scenarios

Overview

IS-IS (Intermediate System to Intermediate System) is a link-state routing protocol used to exchange routing information within an autonomous system (AS). It is commonly used in large service provider and enterprise networks. IS-IS operates at the OSI Layer 2 (data link layer) and Layer 3 (network layer) and is defined in the ISO/IEC 10589 standard.

IS-IS routers exchange information about the network topology by flooding Link State Protocol Data Unit (LSP) throughout the network. Each router builds a map of the network and calculates the best paths to destination networks based on metrics such as link cost.

Key features

Key features of IS-IS include its support for hierarchical routing, fast convergence, scalability, and support for both IPv4 and IPv6 addressing. It is often used in conjunction with other routing protocols like OSPF (Open Shortest Path First) in larger networks.

1. **Hierarchical Design**: IS-IS supports hierarchical routing, dividing the network into areas to scale routing information. This hierarchical structure helps manage network growth and reduce the amount of routing information exchanged between routers.
2. **Link-State Protocol**: IS-IS is a link-state routing protocol, meaning routers exchange information about their directly connected links and the status of those links. This information is flooded throughout the network, allowing each router to build a complete map of the network topology.
3. **Two-Level Hierarchy**: IS-IS employs a two-level hierarchy consisting of Level 1 and Level 2 routing. Level 1 routers exchange routing information within their area, while Level 2 routers exchange routing information between areas.
4. **SPF Algorithm**: IS-IS routers use the Shortest Path First (SPF) algorithm, also known as the Dijkstra algorithm, to calculate the best path to reach destination networks based on link costs. This algorithm ensures efficient path selection and optimal routing.
5. **Addressing Support**: IS-IS supports both IPv4 and IPv6 addressing, making it suitable for networks transitioning to IPv6 or running dual-stack configurations.
6. **Fast Convergence**: IS-IS is known for its fast convergence capabilities, quickly adapting to changes in the network topology and recalculating routes as needed. This helps minimize network downtime and ensures efficient traffic forwarding.
7. **Scalability**: IS-IS is designed to scale to large networks, making it suitable for service provider and enterprise environments with complex network topologies and high traffic volumes.
8. **Authentication**: IS-IS supports authentication mechanisms to secure routing information exchanges between routers, helping prevent unauthorized access and malicious attacks on the network.

IS-IS provides a robust and scalable routing solution for large networks, offering efficient routing, fast convergence, and support for both IPv4 and IPv6 addressing. Its hierarchical design and link-state operation make it well-suited for modern networking environments.

Application Scenarios

IS-IS is a robust link-state routing protocol widely used in large-scale networks. It's particularly favored in service provider and large enterprise environments due to its scalability, flexibility, and rapid convergence. Here are some key application scenarios where IS-IS is particularly effective:

- **Service Provider Networks**

IS-IS can support large-scale networks with thousands of routes, making it ideal for the core backbone of service providers. IS-IS can be used for both Layer 2 (bridging) and Layer 3 (routing) functionalities, providing a versatile solution for Metro Ethernet deployments. Its rapid convergence ensures minimal downtime and quick recovery in the event of link failures, which is crucial for maintaining high availability and reliability.

- **Large Enterprise Networks**

IS-IS supports multi-level hierarchical network design (Level 1 and Level 2), enabling efficient routing in large enterprise networks with multiple branches and campuses. A multinational corporation uses IS-IS to interconnect its global offices, data centers, and remote branches, providing a resilient and scalable routing framework.

- **Data Center Networks**

IS-IS can handle high-throughput environments typical of data centers, ensuring efficient data flow between servers and storage systems. Its simple and flexible configuration options make it suitable for dynamic data center environments where network changes are frequent.

- **Campus Networks**

IS-IS can handle the large number of nodes and devices typically found in campus networks. Many educational and research institutions are early adopters of IPv6, and IS-IS provides a seamless transition from IPv4 to IPv6. For example, a university deploys IS-IS to connect its various buildings, ensuring reliable and efficient communication for academic and administrative purposes.

Configuring IS-IS Basic Function

Only after configuring the basic functions can an IS-IS network be established.

Prerequisites
Configure Network Entity Title (NET)
Enable IS-IS Instance on the Interface
Configure the Level of the IS-IS Switch

NOTEs:

- A maximum of 128 IS-IS routing instances can be configured on a Pica8 switch.
- only up to 3 NETs can be configured.

Prerequisites

Before configuring the basic functions of IS-IS, the following task must be completed:

Configure the IP addresses of the interfaces to ensure network layer reachability between adjacent nodes.

Configure Network Entity Title (NET)

Network Entity Title (NET) is a key component of the addressing scheme. It uniquely identifies each Intermediate System (IS) within the IS-IS routing domain.

The NET consists of three parts:

- Area ID: The length of the Area ID can vary from 1 to 13 bytes.
- System ID: This part has a fixed length of 6 bytes.
- NSAP Selector (SEL): The last byte, different transport protocols correspond to different SELs. For IP, the SEL is always 00.

NOTEs:

- The area address is used to uniquely identify different areas within a routing domain. All switches within the same Level-1 area must have the same area address, while switches within Level-2 areas can have different area addresses.
- Throughout the entire domain and backbone area, it is required to maintain a unique system ID.
- Since a maximum of 3 area addresses can be configured in an IS-IS process, only up to 3 NETs can be configured.

The **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **network-entity** <*network-entity*> command configures network entity title (NET) provided in ISO format. When configuring the NET parameter in IS-IS, ensure that these three components are properly defined according to your network requirements.

Define the IS-IS instance by specifying the **area-tag** <*text*>. This **area-tag** <*text*> helps identify the IS-IS instance on the router.

The following command defines the NET as 32.0001.0040.0220.2030.00. The system ID is 0040.0220.2030 and the region ID is 32.0001.

```
admin@PICOS# set protocols isis area-tag instance1 network-entity 32.0001.0040.0220.2030.00
admin@PICOS# commit
```

Enable IS-IS Instance on the Interface

After configuring the IS-IS instance, to ensure the proper operation of the IS-IS protocol, you also need to enable IS-IS on the link interfaces where IS-IS is running and associate them with the specified instance. The **set protocols isis area-tag** <*text*> **interface** <*interface-name*> <**ipv4-routing | ipv6-routing**> command enables IS-IS instance on a specific L3 interface.

The following command enables IS-IS instance on a specific interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 ipv4-routing
admin@PICOS# commit
```

Configure the Level of the IS-IS Switch

IS-IS switches can be categorized into the following three levels:

- Level-1 switches: Responsible for routing within an area, they only form neighbor relationships with Level-1 and Level-1-2 switches belonging to the same area. Level-1 switches must connect to other areas through Level-1-2 switches.
- Level-2 switches: Responsible for routing between areas, they can form neighbor relationships with Level-2 switches or Level-1-2 switches from other areas. All Level-2 switches constitute the backbone network of the routing domain, facilitating communication between different areas. Level-2 switches within the routing domain must be contiguous to ensure the continuity of the backbone network.
- Level-1-2 switches: They can form Level-1 neighbor relationships with Level-1 and Level-1-2 switches within the same area, as well as Level-2 neighbor relationships with Level-2 and Level-1-2 switches from other areas.

The **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**> command configures the level of the IS-IS switch.

It is advisable for users to complete the configuration of the switch level when configuring IS-IS before network operation.

If the switch level is not specified using this command during the IS-IS configuration process, the router defaults to being a Level-1-2 router. This means it participates in both Level-1 and Level-2 routing calculations, maintaining two LSDBs for Level-1 and Level-2.

The following command configures the level of the IS-IS switch.

```
admin@PICOS# set protocols isis area-tag instance1 is-type level-1
admin@PICOS# commit
```

Configuring IS-IS Authentication

Configuring Authentication for IS-IS Area
Configuring Authentication for IS-IS Routing Domain
Configuring IS-IS Authentication per Interface

IS-IS authentication involves **IS-IS authentication per interface**, **IS-IS area authentication** and **IS-IS routing domain authentication**.

- **IS-IS Authentication per Interface**

IS-IS authentication per interface refers to the interface that enables the IS-IS protocol to authenticate Level 1 and Level 2 Hello messages in a specified manner and password.

- **Area Authentication**

Area authentication encapsulates authentication passwords in IS-IS packets within the Level-1 area, ensuring that only authenticated packets are received. Therefore, when authentication is required for the Level-1 area, IS-IS area authentication needs to be configured on all IS-IS devices within that area.

- **Domain Authentication**

Domain authentication encapsulates authentication passwords in IS-IS packets within the Level-2 area, ensuring that only authenticated packets are received. Therefore, when authentication is required for the Level-2 area, IS-IS domain authentication needs to be configured on all IS-IS devices within that area.

Typically, the IS-IS protocol does not encapsulate authentication information in the sent IS-IS packets, nor does it perform authentication checks on received packets. However, in the event of malicious packet attacks that could lead to the theft of network information, configuring IS-IS authentication can enhance network security.

NOTEs:

- When configuring IS-IS authentication per interface, it is required that the authentication type and password of all devices in the same area or routing domain must be consistent for IS-IS packets to propagate normally.
- Regardless of whether area authentication or routing domain authentication is passed, it does not affect the establishment of Level-1 or Level-2 neighbor relationships.

Configuring Authentication for IS-IS Area

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password**, and all the **area-password** configuration of **authentication-type** and **authentication-key** will be removed.

To configure the authentication type for the IS-IS area, users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password authentication-type** <**simple | md5**>. The authentication type can be **simple** or **md5**.

To configure the authentication password for the IS-IS area, users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password authentication-key** <*password*>. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

By default, IS-IS does not encapsulate authentication information for the sent CSNP and PSNP messages, nor perform authentication checks on the received messages. Users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password authenticate-snp** <**send-only**|**validate**> to change this behavior.

The following commands configure the authentication type, authentication password for the IS-IS area, and configures the system only to encapsulate authentication information for the sent IS-IS messages but will not perform authentication checks on the received messages.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 area-password authenticate-snp send-only
admin@PICOS# commit
```

Configuring Authentication for IS-IS Routing Domain

To configure the authentication type for the IS-IS domain, users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-type** <**simple | md5**>. The authentication type can be **simple** or **md5**.

To configure the authentication password for the IS-IS domain, users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-key** <*password*>.

By default, IS-IS does not encapsulate authentication information for the sent CSNP and PSNP messages, nor perform authentication checks on the received messages. Users can use command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password authenticate-snp** <**send-only**|**validate**> to change this behavior.

The following commands configure the authentication type, authentication password for the IS-IS domain, and configures the system only to encapsulate authentication information for the sent IS-IS messages but will not perform authentication checks on the received messages.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 domain-password authenticate-snp send-only
admin@PICOS# commit
```

Configuring IS-IS Authentication per Interface

Make sure that the authentication configuration per interface on both ends of IS-IS neighbor is consistent, otherwise neighbors cannot be established.

To configure IS-IS authentication type per interface, users can use command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **password authentication-type** <**simple | md5**>. The authentication type can be **simple** or **md5**.

To configure IS-IS authentication password per interface, users can use command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **password authentication-key** <*password*>.

The following commands configure the authentication type, authentication password for the IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-key picos123456
admin@PICOS# commit
```

Configuring LSP Packet Attributes

- Configure the Maximum Size of Generated LSPs
- Configure the Minimum Interval between Regenerating LSP
- Configure the Refresh Period for LSPs
- Configure the Maximum Valid Time for the LSPs

LSP messages are used to exchange link status information. By configuring the basic properties of LSP, the size and maximum valid time of LSP packets can be controlled. It is also possible to adjust the interval between LSP generations, which can enable the network to converge quickly. Additionally, you can configure configuring the refresh period for LSPs to send LSP packets and the refresh cycle of LSP packets.

NOTE:

The LSP maximum lifetime must exceed the refresh interval by more than 300.

Configure the Maximum Size of Generated LSPs

NOTE:

Make sure that the length of the LSP is smaller than the MTU (Maximum Transmission Unit) of the IS-IS interface, otherwise, the LSP messages cannot be sent properly.

When the link state information becomes larger, the length of the generated LSP message can be increased, allowing each LSP to carry more information. Users can control the size of LSP generation and reception through the following commands.

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-mtu** <*max-size*>

The following example configures the maximum size of generated LSPs to 1024 bytes.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-mtu 1024
admin@PICOS# commit
```

Configure the Minimum Interval between Regenerating LSP

When there are changes in local routing information, the device needs to generate new LSPs to announce these changes. When changes in local routing information occur frequently, immediately generating new LSPs consumes a large amount of system resources. To speed up network convergence without affecting system performance, you can adjust the interval between LSP generations using **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers gen-interval** <*lsp-gen-interval*> command.

Configure the Refresh Period for LSPs

The IS-IS network primarily achieves synchronization of link states through the flooding of LSPs. Flooding entails a device sending its LSP to neighbor devices, which then forward the same LSP to all neighbors except the one from which they received it, thus progressively disseminating the LSP throughout the entire hierarchy. This ensures that every device within the hierarchy possesses identical LSP information, thereby maintaining synchronization of the Link State Database (LSDB).

The flooding of LSPs requires periodic refreshing because when a device generates its system LSP, it includes the maximum valid time for the LSP. As other devices receive this LSP, its valid time decreases over time. If a device does not receive an updated LSP, once the valid time of the LSP reaches 0, it will be retained for an additional 60 seconds. If a new LSP is not received within this time, the LSP will be deleted.

Use the command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers refresh-interval** <*lsp-refresh-interval*> to configure the refresh period for LSPs. This interval determines how often the router will re-advertise its LSPs to ensure that other routers in the network have up-to-date information about the network topology. Adjusting this interval can help balance the need for up-to-date information with the desire to minimize unnecessary network traffic.

Configure the Maximum Valid Time for the LSPs

When the switch generates system LSP, the maximum valid time of this LSP will be filled in the LSP. When this LSP is received by other switches, its valid time will continuously decrease over time. If the switch has not received an updated LSP and the valid time of this LSP has decreased to 0, the LSP will remain for another 60 seconds. If a new LSP has not been received yet, it will be deleted.
The **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers max-lifetime** <*lsp-refresh-interval*> command can adjust the maximum valid time of LSP to ensure the validity of old LSP before receiving updated LSP.

Customizing Routes for IS-IS

Configure IS-IS Overload
Configure Attached-bit
Configure Default Metric Value for IS-IS Interface
Configure the Priority for Designated Router Election
Configure IS-IS Passive Interface

Configure IS-IS Overload

There are some circumstances in which it is advantageous to have an IS-IS intermediate system not fully participate in forwarding traffic. For example:

- During startup this intermediate system may be temporarily too busy with the tasks associated with convergence to forward traffic.
- The intermediate system is in a test network that has connections to a production network. The overload bit prevents traffic from moving between the two networks.

You can configure the intermediate system to not forward traffic by enabling the overload bit.

When enabled, the overload bit instructs other intermediate systems not to use this intermediate system as an intermediate hop in their SPF computations. No paths through this intermediate system are visible to other intermediate systems in the domain. IP and CLNS prefixes directly connected to this intermediate system are reachable.

The command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **set-overload-bit** <**true** | **false**> can be used to configure the overload bit for non-pseudonode LSPs.

Configure Attached-bit

The ATT bit is a field in IS-IS LSP (Link State Packet) messages used to indicate whether a Level-1 area is connected to other areas. Level-1-2 routers set this field in their generated Level-1 LSPs to inform Level-1 routers within the same area that they are connected to other areas, specifically to the Level-2 backbone area. When routers in a Level-1 area receive Level-1 LSPs with the ATT bit set from Level-1-2 routers, they create a default route pointing to the Level-1-2 router as the destination, allowing data to be routed to other areas.

The **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **attached-bit send** <**true** | **false**> command can be used to configure whether the Level-1 routers will send default routes in the routing table due to the ATT bit or not.

The following command configures the Level-1 routers to send default routes in the routing table due to the ATT bit.

```
admin@PICOS# set protocols isis area-tag instance1 attached-bit send true
admin@PICOS# commit
```

Configure Default Metric Value for IS-IS Interface

IS-IS uses metrics to determine the best path to a destination. By configuring a default metric value, you influence the path selection process and ensure that traffic follows the desired route.

Configuring different metric values on multiple interfaces can facilitate load balancing. IS-IS can distribute traffic across multiple paths based on their metric values, allowing for efficient utilization of network resources.

The **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **metric** <*metric*> command configures default metric value for IS-IS interface.

If the **metric-style** is not ***wide***, the metric value for IS-IS interface must be less than 64.

The following command configures the default metric value for IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 metric 100
admin@PICOS# commit
```

Configure the Priority for Designated Router Election

Configuring a priority for Designated Router (DR) election in an IS-IS network allows you to influence the selection process for the DR. By assigning different priority values to routers, you can control which routers are more likely to be elected as the DR or BDR. Routers with higher priority values have a greater chance of winning the election.

You can designate certain routers with higher priority values as the preferred DR for critical segments of the network. This ensures that key routers take on leadership roles and helps maintain network stability and performance.

The **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **priority** <*priority*> command configures priority for Designated Router election.

The following command configures the priority for Designated Router election.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 priority 85
admin@PICOS# commit
```

Configure IS-IS Passive Interface

Configuring an layer 3 interface as a passive IS-IS interface prevents the IS-IS process from sending or receiving IS-IS hello packets on the specified interface, effectively making it passive in the IS-IS routing process.

Passive interfaces do not participate actively in IS-IS routing updates. This can be useful in scenarios where you want to limit the exposure of your IS-IS topology to specific interfaces for security reasons.

By marking certain interfaces as passive, you can reduce the amount of IS-IS hello packets exchanged on those interfaces. This can help in conserving network resources and reducing unnecessary control plane traffic.

The **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **passive** command configures the specified layer 3 interface as passive IS-IS interface.

The following command configures the specified layer 3 interface as passive IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 passive
admin@PICOS# commit
```

Configuring IS-IS Timers

- Configuring the Interval for Sending Hello Messages
- Configuring the Hello-Multiplier for the Neighbor Holding Time
- Configuring the Interval for Sending CSNP Messages
- Configuring the Interval for Sending PSNP Messages

Configuring the Interval for Sending Hello Messages

The IS-IS protocol maintains neighbor relationships with neighboring devices through the sending and receiving of Hello messages. When neighboring devices do not receive the Hello message sent by the local end for a period of time, it will be considered that the neighbor has expired. The command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **hello-interval** <*hello-interval*> can be used to specify the interval time for sending Hello messages on an IS-IS interface. The **hello-interval** <*hello-interval*> value is an integer ranging from 1 to 600 seconds. The default value is 3 seconds.

The following commands configure the interval time for sending Hello messages on an IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-interval 30
admin@PICOS# commit
```

Configuring the Hello-Multiplier for the Neighbor Holding Time

The devices at both ends of the link establish a neighbor relationship by sending Hello messages. Once the neighbor relationship is established, periodic Hello messages need to be sent to maintain the neighbor relationship. If the device at one end of the link does not receive the Hello message within a certain interval of time, it is considered that the neighbor has failed. This interval is called neighbor holding time.

For example, if the local device has configured the sending interval of Hello messages to 30 seconds by using command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **hello-interval** <*hello-interval*> , and then using command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **hello-multiplier** <*integer*> to set the multiplier value to 4, the neighbor holding time is 120 seconds (4 * 30=120). When modifying the sending interval of Hello messages, the neighbor holding time also changes accordingly.

The **hello-multiplier** <*integer*> value is an integer ranging from 2 to 100. The default value is 10.

The following commands the interval time for sending Hello messages on an IS-IS interface and configure the multiplier for the interval time between Hello messages. Then the neighbor holding time is 120 seconds (4 * 30=120).

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-interval 30
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-multiplier 4
admin@PICOS# commit
```

Configuring the Interval for Sending CSNP Messages

In an IS-IS broadcasting network, all devices synchronize their Link State Database (LSDB) by periodically broadcasting CSNP (Complete Sequence Number PDU) packets through the Designated Intermediate System (DIS). Upon receiving a CSNP message, if other devices discover that a specific Link State Packet (LSP) is missing from their local LSDB or the locally stored LSP is outdated, they will send a PSNP (Partial Sequence Number PDU) message to request the corresponding LSP. Since only the DIS periodically sends CSNP messages, this command can only be configured on the broadcast network interface of the DIS to be effective. The interval for sending CSNP messages can be adjusted using the **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **csnp-interval** <*csnp-interval*> command. The **csnp-interval** <*csnp-interval*> value is an integer ranging from 1 to 600 seconds. The default value is 10 seconds.

The following commands configure the interval for sending CSNP messages on a broadcast network.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 csnp-interval 50
admin@PICOS# commit
```

Configuring the Interval for Sending PSNP Messages

Partial sequence number message PSNP (Partial SNP): It only lists the sequence numbers of the most recently received LSPs, and can confirm multiple LSPs at once. When it is found that the LSDB is not synchronized, PSNP is also used to request neighbors to send a new LSP. Users can use the command **set protocols isis area-tag** <*text*> **interface** <*interface-name*> **psnp-interval** <*psnp-interval*> to configure the PSNP interval in seconds. The **psnp-interval** <*psnp-interval*> value is an integer ranging from 1 to 120 seconds. The default value is 10 seconds.

The following commands configure the PSNP interval.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 psnp-interval 50
admin@PICOS# commit
```

Controlling IS-IS Routing Information Exchange

Usually, when IS-IS and other routing protocols are deployed in a network, to ensure that traffic from within the IS-IS domain can reach outside the domain, there are typically two approaches:

- Configure edge IS-IS devices to advertise default routes into the IS-IS domain.
- Redistribute routes from other routing domains into IS-IS on edge devices.

You can go to the following pages for detailed information.

- Configuring IS-IS Advertising Default Routes
- Configuring IS-IS Introducing External Routes

Configuring IS-IS Advertising Default Routes

On edge devices with external routes, using the following commands configure to advertise a default route. This allows the device to advertise a default route (0.0.0.0/0) within the IS-IS routing domain.

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **route-map** <*route-map*>

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **always**

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **metric** <*metric*>

If there are multiple edge devices, you can configure a route policy with the parameter **route-map** <*route-map*> to specify the conditions under which a particular edge device should advertise the default route. This helps prevent routing black-holing. Additionally, you can use the parameter **metric** <*metric*> to set the cost value for the default route.

After applying this configuration, other devices within the IS-IS domain will forward traffic destined for external routing domains to this device first. Then, the traffic will be forwarded to the external routing domain through this device.

Configuring IS-IS Introducing External Routes

You can use the following command on the edge devices to introduce routes from other routing domains into IS-IS.

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute** <**ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

When introducing other protocol routes, **route-map** <*route-map*> can be used to only introduce partial routes from other routing domains. Additionally, the configuration parameter **metric** <*metric*> sets the cost value of the introduced route.

You can refer to Configuration Example of Interaction Between IS-IS and BGP to see an example of IS-IS introducing external routes configuration.

Adjusting SPF Calculation Time

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Adjusting SPF (Shortest Path First) calculation time in IS-IS allows for controlling the frequency of route computation when there are changes in the network's link-state database (LSDB). By modifying the SPF calculation time, network administrators can balance between route convergence speed and system resource utilization. If SPF calculation delay is too long, it may slow down route convergence, while if it's too short, it might consume excessive system resources. Adjusting this parameter is crucial for optimizing network performance.

SPF calculation time includes the following parameter configurations:

- **spf-interval:** To configure the interval time for SPF calculation in IS-IS, you can use the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-interval** <*spf-interval*> command. This command allows you to specify the time interval between consecutive SPF calculations. Adjusting this interval can impact route convergence speed and system resource utilization. Here's an example of how to configure it:

```
admin@PICOS# set protocols isis area-tag instance1 spf-interval 60
admin@PICOS# commit
```

- **init-delay:** To configure the initial wait interval before SPF starts after receiving an updated LSA, you can use the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf init-delay** <*init-delay*> command.
- **short-delay** and **long-delay:** To configure the minimum and maximum time between two SPF runs, used to cap the spf holddown value. It also defines how long the network has to be stable before the wait interval is reset to the init-delay and holddown values, you can use the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf short-delay** <*short-delay*> and **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf long-delay** <*long-delay*> commands.
- **holddown:** To configure the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times, you can use the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf holddown** <*holddown*> command.
- **time-to-learn:** To configure the maximum duration typically needed to learn all the IGP events related to a single component failure (such as router failure or SRLG failure), you can use the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf time-to-learn** <*time-to-learn*> command.

Configuration Examples of IS-IS

- Basic IS-IS Configuration Example
- Configuration Example of Interaction Between IS-IS and BGP

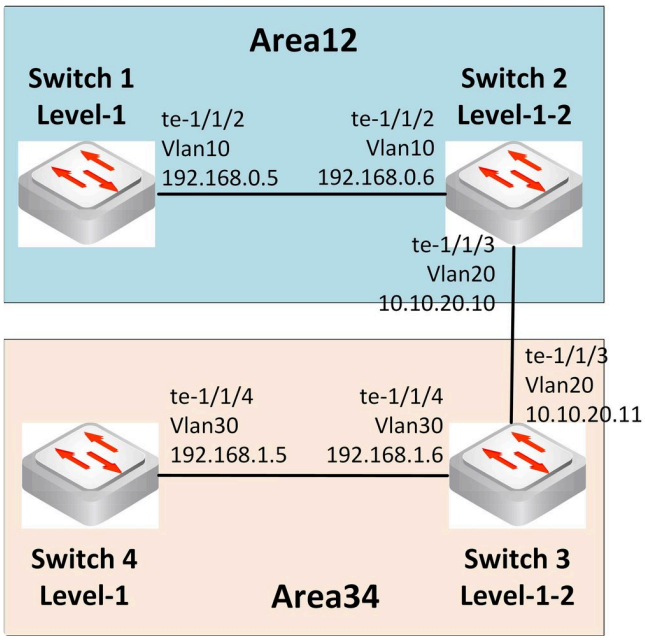
Basic IS-IS Configuration Example

- Network Requirement
- Procedure
  - Switch 1
  - Switch 2
  - Switch 3
  - Switch 4
- Verify the Configuration

Network Requirement

As shown in **Figure 1**, we have four switches. Switch 1 and Switch 2 are in area 12, Switch 3 and Switch 4 in area 34. Switch1 and Switch 4 are intra-area switches so they will be configured as level-1 switches. Switch 2 and Switch 3 form the backbone, so these switches will be configured as level-1-2 switches.

Figure 1. Basic IS-IS Configuration Example



Procedure

This section describes the steps of how to configure basic IS-IS functions on Switch 1, Switch 2, Switch 3 and Switch 4.

Switch 1

Step1 Configure the VLANs and VLAN interfaces.

```
admin@Switch1# set vlans vlan-id 10 l3-interface vlan10
admin@Switch1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 10
admin@Switch1# set l3-interface vlan-interface vlan10 address 192.168.0.5 prefix-length 24
```

Step2 Configure IS-IS basic function.

```
admin@Switch1# set protocols isis area-tag instance1 network-entity 12.0000.0000.0001.00
admin@Switch1# set protocols isis area-tag instance1 is-type level-1
admin@Switch1# set protocols isis area-tag instance1 interface vlan10 ipv4-routing
```

Step3 Enable IP routing.

```
admin@Switch1# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@Switch1# commit
```

Switch 2

Step1 Configure the VLANs and VLAN interfaces.

```
admin@Switch2# set vlans vlan-id 10 l3-interface vlan10
admin@Switch2# set vlans vlan-id 20 l3-interface vlan20
admin@Switch2# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 10
admin@Switch2# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 20
admin@Switch2# set l3-interface vlan-interface vlan10 address 192.168.0.6 prefix-length 24
admin@Switch2# set l3-interface vlan-interface vlan20 address 10.10.20.10 prefix-length 24
```

Step2 Configure IS-IS basic function.

```
admin@Switch2# set protocols isis area-tag instance1 network-entity 12.0001.0000.0000.0002.00
admin@Switch2# set protocols isis area-tag instance1 interface vlan10 ipv4-routing
admin@Switch2# set protocols isis area-tag instance1 interface vlan20 ipv4-routing
```

Step3 Enable IP routing.

```
admin@Switch2# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@Switch2# commit
```

Switch 3

Step1 Configure the VLANs and VLAN interfaces.

```
admin@Switch3# set vlans vlan-id 20 l3-interface vlan20
admin@Switch3# set vlans vlan-id 30 l3-interface vlan30
admin@Switch3# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 20
admin@Switch3# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 30
admin@Switch3# set l3-interface vlan-interface vlan20 address 10.10.20.11 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan30 address 192.168.1.6 prefix-length 24
```

Step2 Configure IS-IS basic function.

```
admin@Switch3# set protocols isis area-tag instance1 network-entity 34.0000.0000.0003.00
admin@Switch3# set protocols isis area-tag instance1 interface vlan20 ipv4-routing
admin@Switch3# set protocols isis area-tag instance1 interface vlan30 ipv4-routing
```

Step3 Enable IP routing.

```
admin@Switch3# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@Switch3# commit
```

Switch 4

Step1 Configure the VLANs and VLAN interfaces.

```
admin@Switch4# set vlans vlan-id 30 l3-interface vlan30
admin@Switch4# set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 30
admin@Switch4# set l3-interface vlan-interface vlan30 address 192.168.1.5 prefix-length 24
```

Step2 Configure IS-IS basic function.

```
admin@Switch4# set protocols isis area-tag instance1 network-entity 34.0000.0000.0004.00
admin@Switch4# set protocols isis area-tag instance1 is-type level-1
admin@Switch4# set protocols isis area-tag instance1 interface vlan30 ipv4-routing
```

Step3 Enable IP routing.

```
admin@Switch4# set ip routing enable true
```

Step4 Commit the configurations.

```
admin@Switch4# commit
```

Verify the Configuration

- View the Link State Database (LSDB) information of IS-IS. Take Switch 1 and Switch 2 as an example. From the result, it can be seen that there are Level-1 and Level-2 Link-State databases on Switch 2.

```
admin@Switch1# run show isis database
Area instance1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *     74   0x00000004  0xa71c     773    0/0/0
    1 LSPs

admin@Switch2# run show isis database
Area instance1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *     84   0x00000005  0x6af2     917    1/0/0
    1 LSPs

IS-IS Level-2 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *     97   0x00000005  0x4785     906    0/0/0
PICOS.00-00               91   0x00000006  0xe911    1134    0/0/0
PICOS.6a-00               51   0x00000001  0xb1ab     677    0/0/0
    3 LSPs
```

- Display IS-IS routing information on switches. Take Switch 2 as an example.

```
admin@Switch2# run show isis route
Area instance1:
IS-IS L1 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop  Label(s)
 -----------------------------------------------------
```

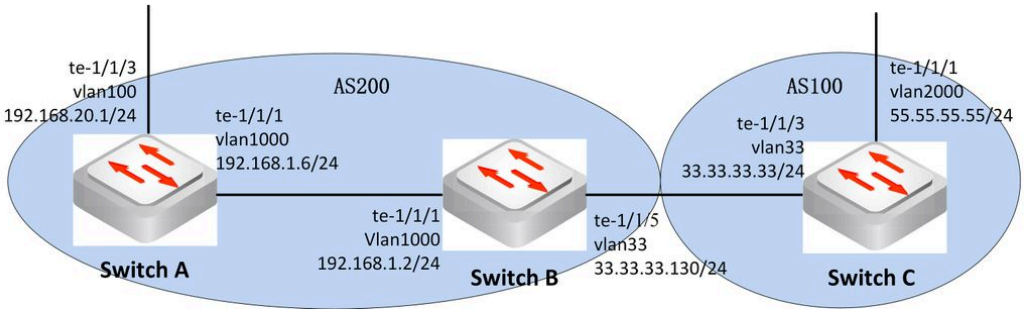
```
 10.10.20.0/24   0       -          -        -
 192.168.0.0/24  0       -          -        -

IS-IS L2 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop      Label(s)
 -----------------------------------------------------------
 10.10.20.0/24   20      vlan20     10.10.20.11  -
 192.168.0.0/24  0       -          -            -
 192.168.1.0/24  20      vlan20     10.10.20.11  -
```

Configuration Example of Interaction Between IS-IS and BGP

Networking Requirements
Procedure
Switch A
Switch B
Switch C
View IS-IS Route Table on Switch A
Configuring Switch B to Import Route between BGP and IS-IS
View IS-IS Route Table on Switch A

Networking Requirements

Figure 1. Configuration Example of Interaction Between IS-IS and BGP



As shown in **Figure 1**, there are three switches (Switch A, Switch B and Switch C) in this sample network. IS-IS routing protocol runs between Switch A and Switch B, and EBGP routing protocol runs between Switch B and Switch C. To enable communication between Switch A and Switch C, you need to configure to redistribute IS-IS routes to BGP routes, and BGP routes to IS-IS routes on Switch B.

Follow the configuration roadmap below to complete the configuration:

1. Configure VLAN interface and IP address for each interface to make the network reachable.
2. Enable IS-IS on Switch A and Switch B, and enable EBGP on Switch B and Switch C.
3. On Switch B, configure route redistribution between route protocol IS-IS and BGP.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 100 l3-interface vlan100
admin@SwitchA# set vlans vlan-id 1000 l3-interface vlan1000
admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 100
admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
admin@SwitchA# set l3-interface vlan-interface vlan100 address 192.168.20.1 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan1000 address 192.168.1.6 prefix-length 24
```

Step2 Enable IS-IS for the network segment.

```
admin@SwitchA# set protocols isis area-tag instance1 network-entity 32.0001.0040.0220.0001.00
admin@SwitchA# set protocols isis area-tag instance1 interface vlan100 ipv4-routing
admin@SwitchA# set protocols isis area-tag instance1 interface vlan1000 ipv4-routing
```

Step3 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 1000 l3-interface vlan1000
admin@SwitchB# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
admin@SwitchB# set interface gigabit-ethernet te-1/1/5 family ethernet-switching native-vlan-id 33
admin@SwitchB# set l3-interface vlan-interface vlan1000 address 192.168.1.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan33 address 33.33.33.130 prefix-length 24
```

Step2 Enable IS-IS for the specified network segment.

```
admin@SwitchB# set protocols isis area-tag instance1 network-entity 32.0001.0040.0220.0002.00
admin@SwitchB# set protocols isis area-tag instance1 interface vlan33 ipv4-routing
admin@SwitchB# set protocols isis area-tag instance1 interface vlan1000 ipv4-routing
```

Step3 Configure EBGP connection between Switch B and Switch C.

```
admin@SwitchB# set protocols bgp local-as 200
admin@SwitchB# set protocols bgp router-id 2.2.2.2
admin@SwitchB# set protocols bgp ebgp-requires-policy false
admin@SwitchB# set protocols bgp ipv4-unicast network 192.168.1.0/24
admin@SwitchB# set protocols bgp neighbor 33.33.33.33 remote-as 100
```

Step4 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step5 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchC# set vlans vlan-id 2000 l3-interface vlan2000
admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 33
admin@SwitchC# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2000
admin@SwitchC# set l3-interface vlan-interface vlan33 address 33.33.33.33 prefix-length 24
admin@SwitchC# set l3-interface vlan-interface vlan2000 address 55.55.55.55 prefix-length 24
```

Step2 Configure EBGP connection between Switch B and Switch C.

```
admin@SwitchC# set protocols bgp local-as 100
```

```
admin@SwitchC# set protocols bgp router-id 3.3.3.3
admin@SwitchC# set protocols bgp ebgp-requires-policy false
admin@SwitchC# set protocols bgp ipv4-unicast network 55.55.55.0/24
admin@SwitchC# set protocols bgp neighbor 33.33.33.130 remote-as 200
```

Step3 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step4 Commit the configuration.

```
admin@SwitchC# commit
```

View IS-IS Route Table on Switch A

- On Switch A, use command **run show isis route** to check IS-IS route table, the route 55.55.55.0/24 does not exist.

```
admin@SwitchA# run show isis route
Area instance1:
IS-IS L1 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop      Label(s)
 ------------------------------------------------------------
 33.33.33.0/24   20      vlan1000   192.168.1.2  -
 192.168.1.0/24  20      vlan1000   192.168.1.2  -

IS-IS L2 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop      Label(s)
 ------------------------------------------------------------
 33.33.33.0/24   20      vlan1000   192.168.1.2  -
 192.168.1.0/24  20      vlan1000   192.168.1.2  -
```

Configuring Switch B to Import Route between BGP and IS-IS

```
admin@SwitchB# set protocols isis area-tag instance1 redistribute ipv4-routing bgp level-1
admin@SwitchB# set protocols isis area-tag instance1 redistribute ipv4-routing bgp level-2
admin@SwitchB# set protocols bgp ipv4-unicast redistribute isis
admin@SwitchB# commit
```

View IS-IS Route Table on Switch A

- On Switch A, use command **run show isis route** to view IS-IS route table again, route 55.55.55.0/24 has been inserted to Switch A's routing table with metric value 10. Switch A and Switch C can communicate with each other now.

```
admin@SwitchA# run show isis route
Area instance1:
IS-IS L1 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop      Label(s)
 ------------------------------------------------------------
 33.33.33.0/24   20      vlan1000   192.168.1.2  -
 55.55.55.0/24   10      vlan1000   192.168.1.2  -
 192.168.1.0/24  20      vlan1000   192.168.1.2  -

IS-IS L2 IPv4 routing table:

 Prefix          Metric  Interface  Nexthop      Label(s)
```

```
-------------------------------------------------------------
33.33.33.0/24   20      vlan1000   192.168.1.2  -
55.55.55.0/24   10      vlan1000   192.168.1.2  -
192.168.1.0/24  20      vlan1000   192.168.1.2  -
```

IP Multicast Routing Configuration

This chapter describes IGMP, PIM-SM, and IGMP snooping configurations.

- IGMP Configuration
- PIM Configuration Guide
  - Introduction of PIM
  - Configuring PIM-SM
  - Example for Configuring PIM-SM
  - Example for Configuring PIM-SSM
  - Example for Configuring PIM over GRE Tunnel
  - RFC List of PIM
  - Example for Configuring Basic PIM-SM
- IGMP Snooping Configuration Guide
  - Introduction to IGMP Snooping
  - Enable Unknown Multicast Traffic Flooding with IGMP Snooping Enabled
  - Configuring IGMP Snooping
  - Example for Configuring Basic IGMP Snooping
  - Example for Configuring IGMP Snooping with IGMP
  - RFC List
- Multicast Source Discovery Protocol (MSDP)
  - Introduction of MSDP
  - Example for Configuring PIM-SM Inter-domain Multicast Using MSDP
  - Example for Configuring Anycast RP
  - RFC Lists of MSDP
- Multicast VLAN Registration (MVR)
  - Overview of MVR
  - Configuration Notes and Constraints of MVR
  - Configuring MVR

IGMP Configuration

In admin@XorPlus, IGMPv1/v2/v3 is supported.

Configuring an IGMP Interface

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan2 address 10.10.60.10 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan3 address 10.10.61.10 prefix-length 24
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set protocols igmp interface vlan2
admin@XorPlus# set protocols igmp interface vlan3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show igmp interface
Interface   State    Address    V   Querier   QuerierIp      QueryTimer   Uptime
vlan2        up     10.10.60.10 2   local     10.10.60.10    00:00:22     00:00:09
vlan3        up     10.10.61.10 2   local     10.10.61.10    --:--:--     00:36:29
```

Configuring IGMP Parameters for the IGMP Interface

```
admin@XorPlus# set protocols igmp interface vlan2 query-interval 4
admin@XorPlus# set protocols igmp interface vlan2 query-max-response-time 100
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring an IGMPv3 Interface

You can configure IGMPv3 in a specified interface.

```
admin@XorPlus# set protocols igmp interface vlan3 version 3
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show igmp interface
Interface State Address     V   Querier QuerierIp    QueryTimer   Uptime
vlan2     up    10.10.60.10 2   local   10.10.60.10  00:00:22     00:00:09
vlan3     up    10.10.61.10 2   local   10.10.61.10  --:--:--     00:36:29
```

Joining and Leaving a Group and Displaying Group Information

If you send an IGMPv2 report to VLAN 2 and an IGMPv3 report to VLAN 3, for example, you can display the group information of the switch. You should not have to worry about 224.0.0.2, 224.0.0.22, etc., which are used for the system (e.g. OSPF, RIP).

```
admin@XorPlus# run show igmp groups
Total IGMP groups: 3
Watermark warn limit(Not Set): 0
```

```
Interface        Group           Mode Timer    Srcs V Uptime
vlan2            224.0.0.2       INCL --:--:--    1 2 01:12:11
vlan2            224.0.0.22      INCL --:--:--    1 2 01:12:11
vlan2            238.255.0.1     INCL --:--:--    1 2 01:12:11
vlan3            224.0.0.2       INCL --:--:--    1 3 01:33:28
vlan3            224.0.0.22      INCL --:--:--    1 3 01:33:28
vlan3            238.255.0.2     INCL --:--:--    1 3 01:33:28
```

If you send a leaving message for the above group, the specified group will be removed.

```
admin@XorPlus# run show igmp groups
Total IGMP groups: 2
Watermark warn limit(Not Set): 0
Interface        Group           Mode Timer    Srcs V Uptime
vlan2            224.0.0.2       INCL --:--:--    1 2 01:22:11
vlan2            224.0.0.22      INCL --:--:--    1 2 01:22:11
vlan3            224.0.0.2       INCL --:--:--    1 3 01:43:28
vlan3            224.0.0.22      INCL --:--:--    1 3 01:43:28
```

PIM Configuration Guide

This section describes how to configure Protocol Independent Multicast (PIM).

> **NOTE:**
> PIM protocol supports VRF.

- Introduction of PIM
- Configuring PIM-SM
- Example for Configuring PIM-SM
- Example for Configuring PIM-SSM
- Example for Configuring PIM over GRE Tunnel
- RFC List of PIM
- Example for Configuring Basic PIM-SM

Introduction of PIM

Protocol Independent Multicast (PIM) as the name suggests, is a multicast routing protocol independent of the unicast routing protocol. It indicates that PIM does not need to maintain dedicated unicast routing information. As a multicast routing solution, it directly uses the routing information of the unicast routing table to perform the Reverse Path Forwarding (RPF) check on the multicast packets. If the RPF check passed, a multicast routing entry and a forwarding table is built for multicast packets forwarding.

As a multicast routing protocol in an IPv4 network, PIM is mainly used to send multicast data streams to multicast devices which is connected to the group members with multicast data requests, implementing route lookup and forwarding of multicast data.

PIM protocol includes two modes: Sparse Mode (PIM-SM) and Dense Mode (PIM-DM). Note that currently, PICOS only supports PIM-SM mode.

This guide provides a brief description and the configuration procedure about PIM-SM in the following section. For details about the working principle of PIM-SM, please refer to RFC standard in 1.4 RFC List.

> **NOTE:**
> - PIM protocol supports VRF.
> - If PIM is configured on a L3 interface added to a VRF, when delete the VRF or the L3 interface after delete PIM, and then roll back to the original configuration, PIM will not work with no multicast routes generated.

PIM Multicast Routing and Forwarding Table

In the implementation of the PIM multicast protocol, two multicast routing forwarding tables including the Multicast Routing Information Base (MRIB) and Multicast Forwarding Table are used for multicast data forwarding.

- **Multicast Routing Information Base (MRIB)**

MRIB in PIM-SM protocol provides the next-hop route along a multicast-capable path to each destination subnet which indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB information. The MRIB is used to determine the next-hop neighbor to which any PIM Join/Prune message is sent. Data flows along the reverse path of the Join messages. You can use **run show pim mrib** command to view the detail information of PIM MRIB.

- **Multicast Forwarding Table**

Multicast Forwarding Table is directly used to control the forwarding of multicast packets. The PIM protocol contains two forwarding entries: (S, G) forwarding entries or (*, G) forwarding entries. S indicates a multicast source, G indicates a multicast group, and * indicates all the Source.

  - The (S, G) forwarding entry is mainly used to build an SPT tree in the PIM network.
  - The (*, G) forwarding entry is mainly used to build an RPT tree in the PIM network.

You can use the **run show pim mfc** command to view the Multicast Forwarding Table information. The information used to guide multicast data forwarding in Multicast Forwarding Table are as follows:

  - Multicast source address.
  - Multicast group address.
  - Incoming interface: The interface on the local router that receives multicast data.
  - Outgoing interfaces: The interface that forwards multicast data out.

Static RP and Dynamic RP

> When the PIM-SM Bootstrap Router mechanism is enabled to dynamically elect an RP, the PICOS switch can receive C-RP advertisement messages sent by other PIM switches. It can then calculate and compare these messages to elect the RP for a specific group from multiple C-RPs. However, the PICOS switch itself does not participate in the election as a BSR or dynamic RP.

Rendezvous Point (RP) is an important PIM-SM router which functions as a conjunction point of the PIM multicast network. RP receives and processes the PIM Register packets from the multicast Source and PIM Join message from the group member to build the PIM Multicast Routing and Forwarding Table for multicast data forwarding.

All PIM routers in the network should know the address of the RP. An RP can serve for multiple multicast Groups at the same time, but a multicast Group can be mapping to one RP. On Pica8 switch, there is two types of RP: static RP and dynamic RP.

- **Static RP**: Statically configured RP by user to specify the location of the RP. The users should configure the same static RP information (including RP address, RP priority and hash mask length) on all PIM-enabled routers in the network.
- **Dynamic RP**: PIM BootStrap Router mechanism is utilized to dynamically elect an RP for the PIM-SM domain. When dynamic RP is deployed, BSR router is responsible for collecting Candidate RP (C-RP) information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM-SM domain. When received the RP-set, each router in the network selects a corresponding RP for a specific multicast group from among multiple C-RPs provided by the RP-Set.

A PIM-SM router must either run the PIM-SM BootStrap Router mechanism to dynamically elect an RP, or have some RPs configured as static RP settings.

Both the static RP and the dynamic RP participate in the RP election if both are configured. PIM routers elects an RP from multiple C-RPs and the static RPs according to the following rules:

1. The C-RP or static RP with highest priority wins.
2. If multiple C-RPs or static RPs have the same priority, the C-RP or static RP with the largest hash value wins.
3. If all the preceding factors are the same, the C-RP or static RP with the largest address wins.

PIM-SM and PIM-SSM

PIM-SM is widely used in large-scale networks with sparsely distributed group members. The key mechanisms of PIM-SM include Neighbor Discovery, DR Election, RP Discovery, RPT Tree Building, Multicast Source Registration, SPT Switchover and Assertion.

PIM Source-Specific Multicast (PIM-SSM) model uses part of the PIM-SM mode technology in practical deployment to provide a solution for source-specific multicast. It maintains the relationship between the host and the router through IGMPv3.

Since the receiver has already known the location of the multicast source in PIM-SSM mode, there is no need for an RP in the SSM model, no need to build an RPT tree, and the multicast source registration process is not required. The PIM-SSM model uses three working mechanisms of PIM-SM: Neighbor Discovery, DR Election and SPT Tree Building to implement multicast forwarding tasks in the PIM domain.

NOTE:

Enable IGMPv3 on the L3 interfaces of the PIM router connected to the receiver when configuring PIM-SSM.

Configuring PIM-SM

Configuration Notes

- Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.
- Currently, only one scope zone is supported, configuring multiple multicast scope zones is not supported.、
- Only PIM-SM and PIM-SSM are supported, PIM-DM is not supported.

Procedure

Step1 Configure Layer 3 interface. PIM-SM can be enabled on VLAN interface or routed interface.

- Configure VLAN interface.

  a) Configure VLAN ID.

  set vlans vlan-id <*vlan-id*>

  b) Configure the interface to VLAN.

  set interface gigabit-ethernet <*port*> **family ethernet-switching native-vlan-id** <*vlan-id*>

  c) Configure the IP address of the VLAN.

  set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>

  d) Associate a Layer 3 interface with a VLAN.

  set vlans vlan-id <vlan-id> **l3-interface** <*interface-name*>

- Configure routed interface.

  a) Enable routed interface.

  set interface gigabit-ethernet <*interface-name*> **routed-interface enable** <**true | false**>

  set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

  b) Configure reserved-vlan for the routed interface.

  set vlans reserved-vlan <*reserved-vlan*>

  c) (Optional) Create the sub-interface and add it into a VLAN.

  set interface aggregate-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

  d) Configure the IP address of the routed interface.

  set l3-interface routed-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix-number*>

Step2 Enable IP routing.

set ip routing enable <**true | false**>

Step3 Enable IGMP on the L3 interfaces of the PIM router connected to the receiver.

set protocols igmp interface <*interface-name*>

Step4 Enable PIM-SM on the L3 interfaces.

set protocols pim interface <*interface-name*> **sm**

Step5 Configure RPs.

> - When both static RP and dynamic RP are configured, the static RP is given priority and selected as the RP.
> - When the PIM-SM Bootstrap Router mechanism is enabled to dynamically elect an RP, the PICOS switch can receive C-RP advertisement messages sent by other PIM switches. It can then calculate and compare these messages to elect the RP for a specific group from multiple C-RPs. However, the PICOS switch itself does not participate in the election as a BSR or dynamic RP.

- Configure static RPs.

  a) Configure the IP address of a static RP.

  set protocols pim rp <*rp-address*>

  b) Assign the group prefix address served by the static RP.

  set protocols pim rp <*rp-address*> **group** <*IPv4Net*>

- Enable dynamic RPs.

  a) Enable the PIM interface to process bootstrap messages.

  set protocols pim interface <*interface-name*> **bsm** <**enable** | **disable**>

  b) Enable the PIM interface to process unicast bootstrap messages.

  set protocols pim interface <*interface-name*> **unicast-bsm** <**enable** | **disable**>

Step6 (Optional) Adjust the PIM protocol parameters in Hello message.

set protocols pim interface <*interface-name*> **drpriority** <*dr-priority*>

set protocols pim interface <*interface-name*> **hello interval**<*interval*>

Step7 (Optional) Configure SPT switchover function.

a) Enable the SPT switchover function.

set protocols pim spt-switchover

b) Configure the SPT Switchover filter list to filter updates to/from this neighbor.

set protocols pim spt-switchover infinity-and-beyond prefix-list <*text*>

Step8 Commit the configurations.

commit

Example for Configuring PIM-SM

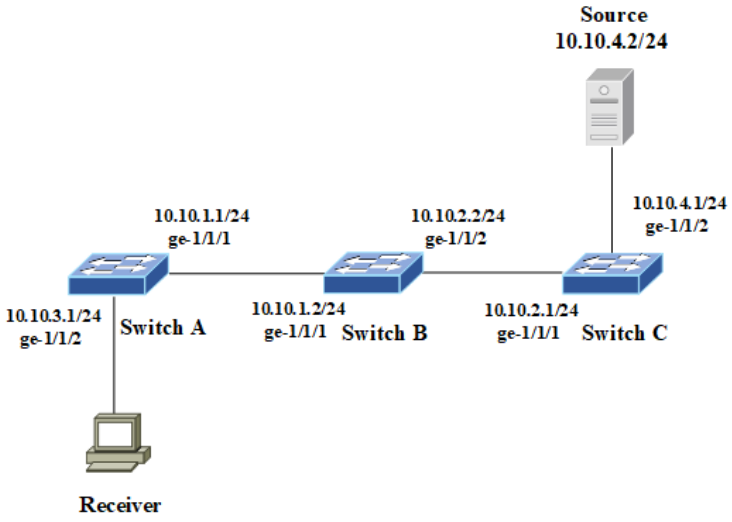
- Networking Requirements
- Procedure
  - Switch A
  - Switch B

Networking Requirements

In the following topology, a multicast Source sends the multicast traffic to the Receiver through Switch C, Switch B and Switch A.

- Configure ge-1/1/2 as an IGMP interface on Switch A which is connected to the Receiver.
- In this example, the static route will be used to make the switches in PIM-SM domain can communicate with each other.

Figure 1. PIM-SM Multicast Routing Configuration



Procedure

Switch A

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.3.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable IGMP on the L3 VLAN interfaces of the PIM router connected to the receiver.

```
admin@XorPlus# set protocols igmp interface vlan-3
```

Step4 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step5 Configure the VLAN interface vlan-2 on Switch A as the static RP.

```
admin@XorPlus# set protocols pim rp 10.10.1.1 group 224.0.0.0/8
```

Step6 Configure static routes to other switches.

```
admin@XorPlus# set protocols static route 10.10.2.0/24 next-hop 10.10.1.2
admin@XorPlus# set protocols static route 10.10.4.0/24 next-hop 10.10.1.2
```

Step7 Commit the configurations.

```
admin@Xorplus# commit
```

Step8 Verify the configuration.

- Run **run show pim interface** command to show information about all interfaces on which PIM-SM is enabled.

```
admin@XorPlus# run show pim interface
Interface         State          Address  PIM Nbrs           PIM DR  FHR IfChannels
vlan-2              up       10.10.1.1         1            local    0          1
vlan-3              up       10.10.3.1         2            local    0          0
```

- Run **run show igmp interface** command to show IGMP interface information.

```
admin@XorPlus# run show igmp interface
Interface State Querier Timeout Version Groups
------------ -------- --------------- --------- --------- --------

vlan-2 DISABLED 10.10.1.1 None 2 0
vlan-3 UP 10.10.3.1 None 2 3

Interface         State          Address  V  Querier  Query Timer    Uptime
vlan-2              up       10.10.1.1    3    local     00:00:40  02:13:12
vlan-3             mtrc      10.10.3.1    3    other     --:--:--  00:36:29
```

Switch B

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.1.2 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.2.2 prefix-length 24
admin@XorPlus# set l3-interface loopback lo address 7.6.5.3 prefix-length 32
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step4 Configure the VLAN interface vlan-2 on Switch A as the static RP.

```
admin@XorPlus# set protocols pim rp 10.10.1.1 group 224.0.0.0/8
```

Step5 Commit the configuration.

```
admin@Xorplus# commit
```

Switch C

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.2.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.4.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step4 Configure the VLAN interface vlan-2 on Switch A as the static RP.

```
admin@XorPlus# set protocols pim rp 10.10.1.1 group 224.0.0.0/8
```

Step5 Configure static routes to other switches.

```
admin@XorPlus#set protocols static route 10.10.1.0/24 next-hop 10.10.2.2
admin@XorPlus#set protocols static route 10.10.3.0/24 next-hop 10.10.2.2
```

Step6 Commit the configuration.

```
admin@Xorplus# commit
```

Step7 Verify the configuration.

- Run **run show pim interface** command to show information about all interfaces on which PIM-SM is enabled.

```
admin@XorPlus# run show pim interface
Interface         State          Address  PIM Nbrs           PIM DR  FHR IfChannels
vlan-2               up       10.10.2.1         0           local    0          1
vlan-3               up       10.10.4.1         0           local    0          0
```

Example for Configuring PIM-SSM

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C

Networking Requirements

PIM-SM is widely used on large-scale networks with sparsely distributed group members. The key mechanisms of PIM-SM include neighbor discovery, DR election, RP discovery, RPT tree building, multicast source registration, SPT switchover and assertion.

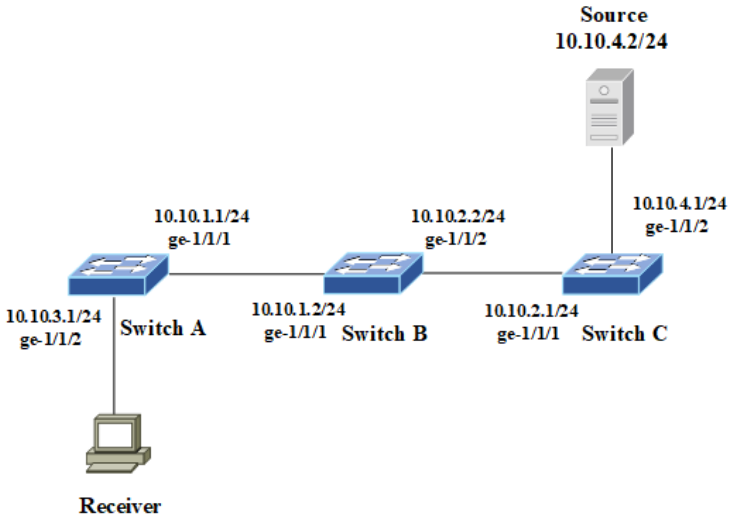
The PIM Source-Specific Multicast (PIM-SSM) model provides a solution for source-specific multicast. It maintains the relationship between the host and the router through IGMPv3 and uses part of the PIM-SM mode technology in practical deployment of the PIM-SSM model.

Since the receiver has already known the location of the multicast source in PIM-SSM mode, there is no need for an RP in the SSM model, no need to build an RPT tree, and the multicast source registration process is not required. The PIM-SSM model uses three working mechanisms: PM-SM neighbor discovery, DR election and SPT tree building to implement multicast forwarding tasks in the PIM domain.

In the following topology, a multicast Source sends the multicast traffic to the Receiver through Switch A, Switch B and Switch C.

- Configure ge-1/1/2 as an IGMPv3 interface on Switch A which connects to the Receiver.
- In this example, the static route in the RIB will be used by PIM-SSM.
- Enable IGMPv3 on the L3 VLAN interfaces of the PIM router connected to the receiver.
- No need for RP configurations in PIM-SSM.

Figure 1. PIM-SSM Multicast Routing Configuration



Procedure

Switch A

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.3.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable IGMPv3 on the L3 VLAN interfaces of the PIM router connected to the receiver.

```
admin@XorPlus# set protocols igmp interface vlan-3 version 3
```

Step4 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step5 Configure static routes to other switches.

```
admin@XorPlus#set protocols static route 10.10.2.0/24 next-hop 10.10.1.2
admin@XorPlus#set protocols static route 10.10.4.0/24 next-hop 10.10.1.2
```

Step6 Commit the configuration.

```
admin@Xorplus# commit
```

Step7 Verify the configuration.

- Run **run show pim interface** command to show information about all interfaces on which PIM-SM is enabled.

```
admin@XorPlus# run show pim interface
Interface         State          Address  PIM Nbrs           PIM DR  FHR IfChannels
vlan-2               up        10.10.1.1         0            local    0          0
vlan-3               up        10.10.3.1         0            local    0          0
```

- Run **run show igmp interface** command to show IGMP interface information.

```
admin@XorPlus# run show igmp interface
Interface         State          Address  V  Querier  Query Timer    Uptime
vlan-2               up        10.10.1.1  3    local     00:00:40  02:13:12
vlan-3             mtrc        10.10.3.1  3    other     --:--:--  00:36:29
```

Switch B

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.1.2 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.2.2 prefix-length 24
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step4 Configure static routes to other switches.

```
admin@XorPlus#set protocols static route 10.10.3.0/24 next-hop 10.10.1.1
admin@XorPlus#set protocols static route 10.10.4.0/24 next-hop 10.10.2.1
```

Step5 Commit the configuration.

```
admin@Xorplus# commit
```

Step6 Verify the configuration.

- Run **run show pim interface** command to show information about all interfaces on which PIM-SM is enabled.

```
admin@XorPlus# run show pim interface
```

```
Interface         State          Address  PIM Nbrs           PIM DR  FHR IfChannels
vlan-2               up        10.10.1.2         0            local    0          0
vlan-3               up        10.10.2.2         0            local    0          0
```

- Run **run show igmp interface** command to show IGMP interface information.

```
admin@XorPlus# run show igmp interface
Interface         State          Address  V  Querier  Query Timer    Uptime
vlan-2               up        10.10.1.2  2    local     00:00:40  02:13:12
vlan-3             mtrc        10.10.2.2  2    other     --:--:--  00:36:29
```

Switch C

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set vlans vlan-id 3 l3-interface vlan-3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 3
admin@XorPlus# set l3-interface vlan-interface vlan-2 address 10.10.2.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan-3 address 10.10.4.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable PIM-SM on the L3 VLAN interfaces.

```
admin@XorPlus# set protocols pim interface vlan-2 sm
admin@XorPlus# set protocols pim interface vlan-3 sm
```

Step4 Configure static routes to other switches.

```
admin@XorPlus#set protocols static route 10.10.1.0/24 next-hop 10.10.2.2
admin@XorPlus#set protocols static route 10.10.3.0/24 next-hop 10.10.2.2
```

Step5 Commit the configuration.

```
admin@Xorplus# commit
```

Step6 Verify the configuration.

- Run **run show pim interface** command to show information about all interfaces on which PIM-SM is enabled.

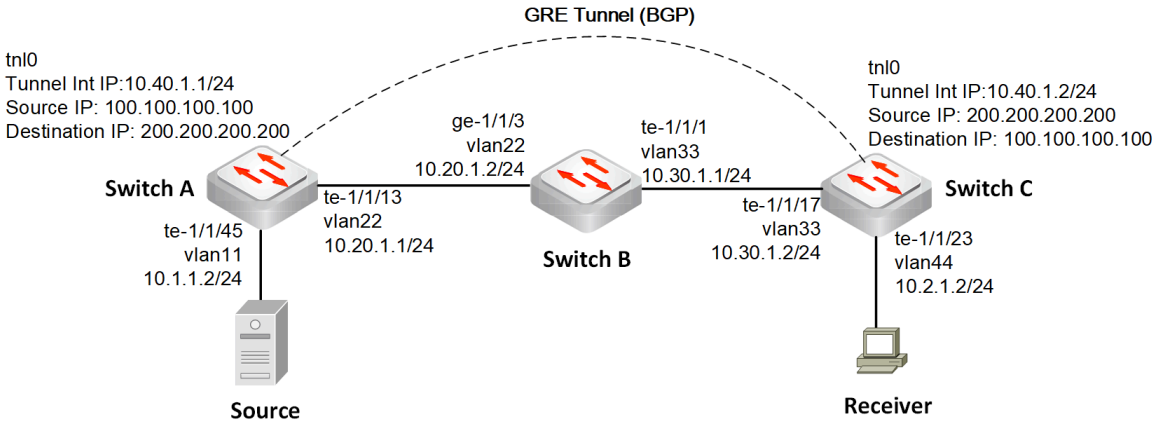
```
admin@XorPlus# run show pim interface
Interface         State          Address  PIM Nbrs           PIM DR  FHR IfChannels
vlan-2               up        10.10.2.1         0            local    0          0
vlan-3               up        10.10.4.1         0            local    0          0
```

Example for Configuring PIM over GRE Tunnel

- Networking Requirements
- Procedure
  - Switch A
  - Switch B
  - Switch C
  - Verifying the Configuration

Networking Requirements

Figure 1. PIM over GRE Tunnel Configuration Example



As shown in **Figure 1**, multicast services are deployed in the network. Switch B does not support multicast protocols, so multicast traffic needs to be transmitted between Switch A and Switch C through a GRE tunnel.

Follow the configuration roadmap below to configure PIM over GRE tunnel.

1. Run OSPF route protocol on Switch A, Switch B and Switch C for underlay communication.
2. Create GRE tunnel interfaces on Switch A and Switch C to establish a GRE tunnel; Run BGP route protocol on GRE tunnel interfaces.
3. Enable PIM function on the GRE tunnel interfaces to enable the transmission of multicast packets by the GRE tunnel.

Procedure

Switch A

Step1 Configure VLAN interface.

```
admin@SwitchA# set vlans vlan-id 11 l3-interface vlan11
admin@SwitchA# set vlans vlan-id 22 l3-interface vlan22
admin@SwitchA# set interface gigabit-ethernet te-1/1/45 family ethernet-switching native-vlan-id 11
admin@SwitchA# set interface gigabit-ethernet te-1/1/13 family ethernet-switching native-vlan-id 22
admin@SwitchA# set l3-interface loopback lo address 100.100.100.100 prefix-length 32
admin@SwitchA# set l3-interface vlan-interface vlan11 address 10.1.1.2 prefix-length 24
admin@SwitchA# set l3-interface vlan-interface vlan22 address 10.20.1.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@SwitchA# set ip routing enable true
```

Step3 Configure OSPF route protocol for underlay communication.

```
admin@SwitchA# set protocols ospf router-id 1.1.1.1
admin@SwitchA# set protocols ospf network 10.20.1.0/24 area 0
admin@SwitchA# set protocols ospf network 100.100.100.100/32 area 0
```

Step4 Configure GRE tunnel name, IP, source IP, destination IP etc.

```
admin@SwitchA# set l3-interface tunnel tnl0 address 10.40.1.1 prefix-length 24
admin@SwitchA# set l3-interface tunnel tnl0 tunnel-mode gre-ip
```

```
admin@SwitchA# set l3-interface tunnel tnl0 source 100.100.100.100
admin@SwitchA# set l3-interface tunnel tnl0 destination 200.200.200.200
```

Step5 Configure BGP route protocol for the GRE tunnel.

```
admin@SwitchA# set protocols bgp local-as 100
admin@SwitchA# set protocols bgp ebgp-requires-policy false
admin@SwitchA# set protocols bgp neighbor 10.40.1.2 remote-as 200
admin@SwitchA# set protocols bgp ipv4-unicast network 10.1.1.0/24
```

Step6 Enable PIM on the GRE tunnel interface, configure Switch A's GRE tunnel interface as the static RP.

```
admin@SwitchA# set protocols pim interface vlan11 sm
admin@SwitchA# set protocols pim interface tnl0 sm
admin@SwitchA# set protocols pim rp 10.40.1.1 group 225.0.0.0/8
```

Step7 Commit the configuration.

```
admin@SwitchA# commit
```

Switch B

Step1 Configure VLAN interface.

```
admin@SwitchB# set vlans vlan-id 22 l3-interface vlan22
admin@SwitchB# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchB# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 22
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 33
admin@SwitchB# set l3-interface vlan-interface vlan22 address 10.20.1.2 prefix-length 24
admin@SwitchB# set l3-interface vlan-interface vlan33 address 10.30.1.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@SwitchB# set ip routing enable true
```

Step3 Configure OSPF for the connections between Switch A, Switch B and Switch C.

```
admin@SwitchB# set protocols ospf router-id 2.2.2.2
admin@SwitchB# set protocols ospf network 10.30.1.0/24 area 0
admin@SwitchB# set protocols ospf network 10.20.1.0/24 area 0
```

Step4 Commit the configuration.

```
admin@SwitchB# commit
```

Switch C

Step1 Configure VLAN interface.

```
admin@SwitchC# set vlans vlan-id 33 l3-interface vlan33
admin@SwitchC# set vlans vlan-id 44 l3-interface vlan44
admin@SwitchC# set interface gigabit-ethernet te-1/1/17 family ethernet-switching native-vlan-id 33
admin@SwitchC# set interface gigabit-ethernet te-1/1/23 family ethernet-switching native-vlan-id 44
admin@SwitchC# set l3-interface loopback lo address 200.200.200.200 prefix-length 32
admin@SwitchC# set l3-interface vlan-interface vlan33 address 10.30.1.2 prefix-length 24
admin@SwitchC# set l3-interface vlan-interface vlan44 address 10.2.1.2 prefix-length 24
```

Step2 Enable IP routing.

```
admin@SwitchC# set ip routing enable true
```

Step3 Configure OSPF routes for underlay communication.

```
admin@SwitchC# set protocols ospf router-id 3.3.3.3
admin@SwitchC# set protocols ospf network 10.30.1.0/24 area 0
```

```
admin@SwitchC# set protocols ospf network 200.200.200.200 area 0
```

Step4 Configure GRE tunnel name, IP, source IP, destination IP etc.

```
admin@SwitchC# set l3-interface tunnel tnl0 address 10.40.1.2 prefix-length 24
admin@SwitchC# set l3-interface tunnel tnl0 tunnel-mode gre-ip
admin@SwitchC# set l3-interface tunnel tnl0 source 200.200.200.200
admin@SwitchC# set l3-interface tunnel tnl0 destination 100.100.100.100
```

Step5 Configure BGP routes for the GRE tunnel.

```
admin@SwitchC# set protocols bgp local-as 200
admin@SwitchC# set protocols bgp ebgp-requires-policy false
admin@SwitchC# set protocols bgp neighbor 10.40.1.1 remote-as 100
admin@SwitchC# set protocols bgp ipv4-unicast network 10.2.1.0/24
```

Step6 Enable PIM on the GRE tunnel interface, configure Switch A's GRE tunnel interface as the static RP.

```
admin@SwitchC# set protocols pim interface vlan33 sm
admin@SwitchC# set protocols pim interface tnl0 sm
admin@SwitchC# set protocols pim rp 10.40.1.1 group 225.0.0.0/8
```

Step7 Configure the IGMP function of the connected receiver interface.

```
admin@SwitchC# set protocols igmp interface vlan44
```

Step8 Commit the configuration.

```
admin@SwitchC# commit
```

Verifying the Configuration

- After the configuration is complete, run **run show pim interface** to view the configuration and operation state of PIM on an interface.

```
admin@switchA# run show pim interface
Interface  State   Address     PIM Nbrs  PIM DR       FHR  IfChannels
 tnl0       up     10.40.1.1   1         10.40.1.2    0    2
 pimreg     up     0.0.0.0     0         local        0    0
 vlan11     up     10.1.1.2    0         local        0    0

admin@switchC# run show pim interface
Interface   State  Address      PIM Nbrs  PIM DR  FHR  IfChannels
 tnl0       up     10.40.1.2    1         local   0    0
 pimreg     up     0.0.0.0      0         local   0    0
 vlan44     up     10.2.1.2     0         local   0    2
```

- Run command **run show l3-interface tunnel** to display information about the GRE tunnel interface.

```
admin@SwitchA# run show l3-interface tunnel tnl0
tnl0        State:UP
            Tunnel Source: 100.100.100.100
            Tunnel Destnation: 200.200.200.200
            Tunnel protocol/transport: gre-ip
            Inet addr: 10.40.1.1
            Traffic statistics:
              5 sec input rate IPv4 1200 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 80 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................28
              IPv4 Forwarding Packets.....................5
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets.....................0
```

- Run commands **run show pim neighbor and run show pim rp-info** to that the PIM neighbor information and RP information have been generated correctly.

```
admin@switchA# run show pim neighbor
Interface  Neighbor     Uptime    Holdtime  DR Pri
tnl0       10.40.1.2    03:10:40  00:01:34  1
```

```
admin@switchA# run show pim rp-info
RP address   group/prefix-list  OIF        I am RP  Source  Group-Type
10.40.1.1    225.0.0.0/8       tnl0       yes      Static   ASM
```

- In this example, multicast source 10.1.1.5 sends multicast information to multicast group 225.0.0.2. The multicast routing table generated by PIM protocol can be viewed through the **run show mroute** command, which shows that multicast traffic can be transmitted through the GRE tunnel.

```
admin@switchA# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - SGRpt Pruned, F - Register flag, T - SPT-bit set
 Source     Group      Flags   Proto  Input      Output     TTL  Uptime
 *          225.0.0.2   S      none   tnl0       none       0    --:--:--
 10.1.1.5   225.0.0.2   SFT    PIM    vlan11     pimreg     1    02:59:50
                               STAR              tnl0       1

admin@switchC# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - SGRpt Pruned, F - Register flag, T - SPT-bit set
 Source     Group      Flags   Proto    Input      Output  TTL  Uptime
 *          225.0.0.2  SC      IGMP     tnl0       pimreg  1    03:07:44
                               IGMP               vlan44  1
 10.1.1.5   225.0.0.2  ST      STAR     tnl0       vlan44  1    03:07:17
```

RFC List of PIM

The following table lists the RFC documents related to PIM protocol.

RFC	Description
RFC3569	An Overview of Source-Specific Multicast (SSM)
RFC4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC5059	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
RFC4607	Source-Specific Multicast for IP

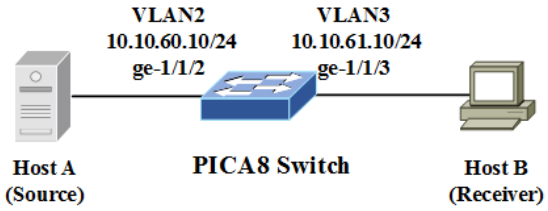
Example for Configuring Basic PIM-SM

- Networking Requirements
- Procedure
  - Host A (Source)
  - Host B (Receiver)
  - PICA8 Switch
- Verify the Configuration
- Verify End to End Connectivity between Host A and Host B

Networking Requirements

As shown in **Figure 1**, Host B wants to receive multicast data from Host A (Source) through the Pica8 Switch.

Figure1. User Configuration Topology of PIM-SM



Follow the configuration roadmap below to complete the configuration on PICA8 Switch.

1. Create the L3 VLAN interfaces.
2. Enable IGMP on the L3 VLAN interfaces.
3. Enable PIM-SM on L3 VLAN interfaces.

Procedure

Host A (Source)

- Add route on Host A to reach Host B.

  For example, use the following command on Linux system,

  sudo route add default gw 10.10.60.10 eth1

- Run iPerf on Host A.

Host B (Receiver)

- Add route on Host B to reach Host A.

  For example, use the following command on Linux system,

  sudo route add default gw 10.10.61.10 eth1

- Run iPerf on Host B.

PICA8 Switch

Step1 Create the L3 VLAN interfaces and assign VLAN to ports.

```
admin@Xorplus# set vlans vlan-id 2 l3-interface vlan2
admin@Xorplus# set l3-interface vlan-interface vlan2 address 10.10.60.10 prefix-length 24
admin@Xorplus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@Xorplus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
```

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 3
admin@Xorplus# set vlans vlan-id 3 l3-interface vlan3
admin@Xorplus# set l3-interface vlan-interface vlan3 address 10.10.61.10 prefix-length 24
admin@Xorplus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@Xorplus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@Xorplus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 2
```

Step2 Enable IP routing.

```
admin@Xorplus# set ip routing enable true
```

Step3 Enable IGMP on the L3 VLAN interfaces.

```
admin@Xorplus# set protocols igmp interface vlan2
admin@Xorplus# set protocols igmp interface vlan3
```

Step4 Enable PIM on the L3 VLAN interfaces and assign the group ID.

```
admin@Xorplus# set protocols pim interface vlan2 sm
admin@Xorplus# set protocols pim interface vlan3 sm
admin@Xorplus# set protocols pim rp 10.10.60.10 group 226.0.0.0/8
admin@Xorplus# set protocols pim rp 10.10.61.10 group 226.0.0.0/8
```

Step5 Configure the log level.

```
admin@Xorplus# set protocols pim traceoption trace
admin@Xorplus# set protocols igmp traceoption trace
admin@Xorplus# set system log-level trace
```

Step6 Commit the configurations.

```
admin@Xorplus# commit
```

Verify the Configuration

- Run the **run show igmp interface** command to check the IGMP interface configuration.

```
admin@XorPlus# run show igmp interface
Interface         State          Address  V  Querier          QuerierIp  Query Timer    Uptime
vlan2               up      10.10.60.10  3    local        10.10.60.10     00:00:14  00:04:28
vlan3               up      10.10.61.10  3    local        10.10.61.10     00:00:14  00:04:28
```

- Run the **run show pim interface** command to check the PIM configuration and status.

```
admin@Xorplus# run show pim interface
Interface  State  Address      PIM Nbrs  PIM DR  FHR  IfChannels
 pimreg     up     0.0.0.0      0         local   0    0
 vlan2      up     10.10.60.10  0         local   0    0
 vlan3      up     10.10.61.10  0         local   0    0
```

- - Run the **run show l3-interface brief** command to check the VLAN interface configuration.

```
admin@XorPlus# run show l3-interface brief
Interface          Vlan ID    Status    Addr                                        Description
---------------    -------    ------    ----------------------------------------    ---------------------------------------
vlan2              2          UP        10.10.60.10/24
                                        fe80::e81:3e20:15c:0/64
vlan3              3          UP        10.10.61.10/24
                                        fe80::e81:3e20:25c:0/64
```

- Run the **run show igmp group** command to show information about multicast group member ports.

```
admin@XorPlus# run show igmp groups
Interface        Group           Mode Timer    Srcs V Uptime
vlan2            224.0.0.2       INCL --:--:--    1 2 01:33:28
vlan2            224.0.0.13      INCL --:--:--    1 2 01:33:28
vlan2            224.0.0.22      INCL --:--:--    1 2 01:33:25
vlan3            224.0.0.2       INCL --:--:--    1 2 00:33:12
vlan3            224.0.0.13      INCL --:--:--    1 2 00:33:12
vlan3            224.0.0.22      INCL --:--:--    1 2 00:33:09
```

Verify End to End Connectivity between Host A and Host B

- Connectivity between Host A and Host B.

```
th1
net  HWaddr 00:1b:21:1e:f2:19
61.11  Bcast:10.10.61.255  Mask:255.255.255.0
::21b:21ff:fe1e:f219/64 Scope:Link
NING MULTICAST  MTU:1500  Metric:1
105113 errors:682531 dropped:2810721675 overruns:0 fra

57371 errors:0 dropped:0 overruns:0 carrier:0
ueuelen:1000
688786 (7.1 TB)  TX bytes:545967719341 (545.9 GB)
ory:f0200000-f0220000

.60.11
.11) 56(84) bytes of data.
 icmp_seq=3 ttl=63 time=0.159 ms
 icmp_seq=6 ttl=63 time=0.172 ms
 icmp_seq=7 ttl=63 time=0.125 ms
 icmp_seq=8 ttl=63 time=0.174 ms
 icmp_seq=9 ttl=63 time=0.188 ms
```

```
sharad@upc-2:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:1b:21:35:62:e
          inet addr:10.10.60.11  Bcast:10.10.60.255  M
          inet6 addr: fe80::21b:21ff:fe35:62ec/64 Scop
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Me
          RX packets:33414837036 errors:334625 dropped
ame:334623
          TX packets:1636886920 errors:0 dropped:0 ove
          collisions:0 txqueuelen:1000
          RX bytes:2411294716327 (2.4 TB)  TX bytes:21
          Interrupt:16 Memory:f0680000-f06a0000

sharad@upc-2:~$ ping 10.10.61.11
PING 10.10.61.11 (10.10.61.11) 56(84) bytes of data.
64 bytes from 10.10.61.11: icmp_seq=2 ttl=63 time=0.18
64 bytes from 10.10.61.11: icmp_seq=6 ttl=63 time=0.19
64 bytes from 10.10.61.11: icmp_seq=7 ttl=63 time=0.18
64 bytes from 10.10.61.11: icmp_seq=8 ttl=63 time=0.19
```

- IPerf result from Host A to Host B.

```
 -c 226.94.1.1 -u -T 32 -t 15 -i 1
------------------------------------
.1.1, UDP port 5001


 (default)
------------------------------------
t 48751 connected with 226.94.1.1 port 5001
er     Bandwidth
Bytes  1.06 Mbits/sec
Bytes  1.05 Mbits/sec
Bytes  1.05 Mbits/sec
Bytes  1.05 Mbits/sec
Bytes  1.05 Mbits/sec
 KBytes  1.05 Mbits/sec
```

```
sharad@upc-2:~$
sharad@upc-2:~$ sudo iperf -s -u -B 226.94.1.1 -i 1
[sudo] password for sharad:
------------------------------------------------------------
Server listening on UDP port 5001
Binding to local address 226.94.1.1
Joining multicast group  226.94.1.1
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 226.94.1.1 port 5001 connected with 10.10.6
[ ID] Interval       Transfer     Bandwidth        Jitt
[  3]  0.0- 1.0 sec   128 KBytes  1.05 Mbits/sec   0.00
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec   0.00
[  3]  2.0- 3.0 sec   129 KBytes  1.06 Mbits/sec   0.00
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec   0.00
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec   0.00
[  3]  0.0- 5.5 sec   709 KBytes  1.05 Mbits/sec   0.00
```

- IPerf result from Host B to Host A.

```
'f -s -u -B 226.94.1.1 -i 1
------------------------------------
ort 5001
 226.94.1.1
 226.94.1.1
rams
rte (default)
------------------------------------
ort 5001 connected with 172.16.0.96 port 44677
nsfer     Bandwidth        Jitter   Lost/Total Datagrams
 KBytes  1.05 Mbits/sec   0.002 ms    0/   89 (0%)
 KBytes  1.05 Mbits/sec   0.002 ms    0/   89 (0%)
 KBytes  1.05 Mbits/sec   0.002 ms    0/   89 (0%)
 KBytes  1.05 Mbits/sec   0.002 ms    0/   89 (0%)
 KBytes  1.05 Mbits/sec   0.002 ms    0/   89 (0%)
 KBytes  1.06 Mbits/sec   0.001 ms    0/   90 (0%)
 KBytes  1.05 Mbits/sec   0.001 ms    0/   89 (0%)
 KBytes  1.05 Mbits/sec   0.002 ms    0/  713 (0%)
```

```
sharad@upc-2:~$
sharad@upc-2:~$ sudo  iperf -c 226.94.1.1 -u -T 32 -t
------------------------------------------------------------
Client connecting to 226.94.1.1, UDP port 5001
Sending 1470 byte datagrams
Setting multicast TTL to 32
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 172.16.0.96 port 44677 connected with 226
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 1.0 sec   129 KBytes  1.06 Mbits/sec
[  3]  1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  3.0- 4.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  5.0- 6.0 sec   128 KBytes  1.05 Mbits/sec
[  3]  6.0- 7.0 sec   129 KBytes  1.06 Mbits/sec
^C[  3]  0.0- 8.0 sec  1024 KBytes  1.05 Mbits/sec
[  3] Sent 713 datagrams
sharad@upc-2:~$
```

IGMP Snooping Configuration Guide

- Introduction to IGMP Snooping
- Enable Unknown Multicast Traffic Flooding with IGMP Snooping Enabled
- Configuring IGMP Snooping
- Example for Configuring Basic IGMP Snooping
- Example for Configuring IGMP Snooping with IGMP
- RFC List

Introduction to IGMP Snooping

IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. If the switch does not run IGMP snooping, it broadcasts multicast packets at Layer 2. However, if IGMP snooping is enabled, switch forwards multicast packets only to specified host ports based on the Layer 2 multicast forwarding table.

IGMP snooping is a basic Layer 2 multicast function that forwards and controls the link layer multicast data. IGMP snooping runs on a Layer 2 multicast device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 multicast device forwards multicast packets based on this Layer 2 multicast forwarding table.

After a Layer 2 multicast forwarding table is set up, the Layer 2 multicast device searches the multicast forwarding table for outbound ports of multicast data packets according to the VLAN IDs and destination addresses (group addresses) of the packets. If there is an outbound port for the multicast data packet, the Layer 2 multicast device forwards the packet to the corresponding multicast group member port. If no outbound port is found, the multicast data packet will be dropped by the Layer 2 multicast device. However, the unknown multicast packet can be forwarded to other router ports except the one receiving the packet.

For more information about IGMP snooping, please refer to RFC 4541.

NOTE:

- PICOS supports IGMP snooping of IGMPv1, IGMPv2 and part of IGMPv3. However, PICOS supports IGMPv3 snooping without considering the additional "include source" or "exclude source" filtering in the packets. For example,
  - When receiving an IGMPv3 snooping report message, the switch parses the packet and records the member port and the multicast group as a Layer 2 forwarding entry without parsing and recording the particular source information.
  - When receiving an IGMPv3 snooping general query packet, the switch parses the packet and records the corresponding router port information. The original packet is then forwarded.
- The report message from the downstream hosts will be treated as IGMPv3 message only when the destination address is 224.0.0.22.
- If the report message from the downstream hosts is IGMPv3 message (Type value is 0x22), but the destination address in the message is not 224.0.0.22, PICOS will not record this member port to the Layer 2 forwarding table.
- In L2/L3, IGMPv2/IGMPv3 Snooping and IGMPv2 Snooping Querier are both supported.
- When the switch receives an unknown multicast, it will forward the data packet to the router port. The unknown multicast data packet refers to multicast data packets that do not exist in the IGMP snooping forwarding table.

Enable Unknown Multicast Traffic Flooding with IGMP Snooping Enabled

Background

When IGMP snooping is enabled, unknown multicast traffic can only be forwarded to the router ports by default. This causes the loss of protocol packets like mDNS or legacy protocols like AppleTalk since packets are not flooded to all ports of the VLAN. To solve this problem, users can enable the function of unknown multicast traffic flooding in a VLAN with IGMP snooping enabled.

The following command can be used:

set protocols igmp-snooping vlan-id <*vlan-id*> **unregistered flood-all** <**true | false**>

When set to true, the function is enabled. Unknown multicast traffic can be flooded to all the ports in a VLAN with IGMP snooping enabled.

This function is disabled by default. Unknown multicast traffic can be forwarded to the router ports.

Examples

- Enable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 100 unregistered flood-all true
admin@Xorplus# commit
```

- Disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 100 unregistered flood-all false
admin@Xorplus# commit
```

Configuring IGMP Snooping

Procedure

Step1 Enable the global IGMP snooping function.

set protocols igmp-snooping enable <**true** | **false**>

Step2 Enable the VLAN-based IGMP snooping function.

set protocols igmp-snooping vlan-id <*vlan-id*> **enable** <**true** | **false**>

NOTE:

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Step3 Configure the number of times that the querier sends a group-specific query message.

set protocols igmp-snooping last-member-query-count <*last-member-query-count*>

Step4 Configure the interval that the querier sends a group-specific query message.

set protocols igmp-snooping last-member-query-interval <*last-member-query-interval*>

Step5 Configure the maximum response time for IGMP general query message.

set protocols igmp-snooping max-response-time <*max-response-time*>

Step6 Configure the interval of sending IGMP general queries.

set protocols igmp-snooping query-interval <*query-interval*>

Step7 Enable the membership report suppression function.

set protocols igmp-snooping report-suppression <**true | false**>

Step8 Configure the IGMP robustness coefficient.

set protocols igmp-snooping robustness-variable <*robustness-variable*>

Step9 Configure the aging time of dynamic router port.

set protocols igmp-snooping router-aging-time <*router-aging-time*>

Step10 Enable the fast leave function to allow member ports in a VLAN to quickly leave the multicast group.

set protocols igmp-snooping vlan-id <*vlan-id*> **fast-leave** <**true | false**>

Step11 Configure the querier in a VLAN.

a) Enable the querier function in a VLAN.

set protocols igmp-snooping vlan-id <*vlan-id*> **querier enable** <**true | false**>

b) Configure the IGMP snooping querier IP address.

set protocols igmp-snooping vlan-id <*vlan-id*> **querier address** <*querier-address*>

c) Configure the IGMP snooping querier version.

set protocols igmp-snooping vlan-id <*vlan-id*> **querier version** <*querier-version*>

d) Configure the IGMP snooping querier other-querier-timer.

set protocols igmp-snooping vlan-id <*vlan-id*> **querier other-querier-timer** <*other-querier-timer*>

Step12 Configure the interface as a static router port in the specified VLAN.

set protocols igmp-snooping vlan-id <*vlan-id*> **mrouter interface** <*interface-name*>

Step13 Configure a static member interface to the multicast group.

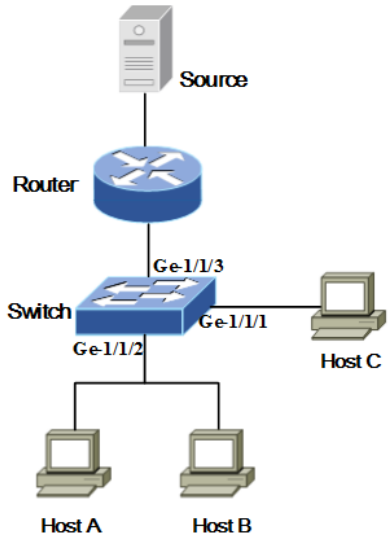
set protocols igmp-snooping vlan-id <*vlan-id*> **static group** <*group-address*> **interface** <*interface-name*>

Example for Configuring Basic IGMP Snooping

- Networking Requirments
- Procedure
- Verify the Configuration

Networking Requirments

Figure 1. IGMP Snooping Networking



As shown in Figure 1, Host A, Host B, and Host C connect to a multicast source through a Layer 2 Switch and a Layer 3 Router to receive multicast data from the Source device.

Perform the following procedures on the Switch to implement IGMP snooping:

- Create a VLAN and add interfaces Ge-1/1/1, Ge-1/1/2 and Ge-1/1/3 to the VLAN.
- Enable global and VLAN-based IGMP snooping function.
- Host C wants to receive multicast data from multicast group 238.255.0.1 stably for a long time, so configure the connecting interface Ge-1/1/1 as a static member port.
- To prevent aging of dynamic routing interfaces, configure Ge-1/1/3 as a static router port.

Procedure

Step1 Configure VLAN.

```
admin@XorPlus# set vlans vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 2
```

Step2 Enable the global IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping enable true
```

Step3 Enable the VLAN-based IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 enable true
```

NOTE:

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Step4 (Optional) Configure the number of times that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-count 2
```

Step5 (Optional) Configure the interval that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-interval 2
```

Step6 (Optional) Configure the maximum response time for IGMP general queries.

```
admin@Xorplus# set protocols igmp-snooping max-response-time 10
```

Step7 (Optional) Configure the interval of sending an IGMP general queries.

```
admin@Xorplus# set protocols igmp-snooping query-interval 60
```

Step8 (Optional) Enable the membership report suppression function.

```
admin@Xorplus# set protocols igmp-snooping report-suppression true
```

Step9 (Optional) Configure the IGMP robustness coefficient.

```
admin@Xorplus# set protocols igmp-snooping robustness-variable 2
```

Step10 (Optional) Configure aging time of dynamic router port.

```
admin@Xorplus# set protocols igmp-snooping router-aging-time 260
```

Step11 (Optional) Enable the fast leave function to allow member ports in a VLAN to quickly leave the multicast group.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 fast-leave true
```

Step12 (Optional) Configure the querier in the VLAN.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 querier enable true
admin@Xorplus# set protocols igmp-snooping vlan-id 2 querier address 192.168.12.100
admin@Xorplus# set protocols igmp-snooping vlan-id 2 querier version 2
admin@Xorplus# set protocols igmp-snooping vlan-id 2 querier other-querier-timer 120
```

Step13 Configure the interface as a static router port in the specified VLAN.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 mrouter interface ge-1/1/3
```

Step14 Configure a static member interface to the multicast group.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 static group 238.255.0.1 interface ge-1/1/1
```

Verify the Configuration

- You can use the **run show igmp-snooping** command to view the configuration information of IGMP snooping.

```
admin@XorPlus# run show igmp-snooping
Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping             : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Router aging time            : 260
Max response time            : 10
Query interval               : 60
Last member query count      : 2
Last member query interval    : 2


admin@XorPlus# run show igmp-snooping vlan 2
Vlan 2:
```

```
-------------------------------------------
IGMP snooping                    : Enabled
IGMPv2 fast leave                  : Enabled
IGMP querier state                  : Enabled
IGMP querier source ip address        : 192.168.12.100
IGMP other querier timer             : 120
IGMP querier version                : 2
```

- You can use the run show igmp-snooping groups command to show information about multicast group member ports which is used for Layer 2 forwarding, namely, the Layer 2 forwarding table.

```
admin@XorPlus# run show igmp-snooping groups
Vlan      Group                Port List          Type
--------  ------------------      -----------------   ----------------------
 2      238.255.0.1              ge-1/1/1           Static
                                   ge-1/1/3           Mrouter
```

- You can use the **runshow igmp-snooping querier** command to show the configuration information and status of the querier.

```
admin@XorPlus# run show igmp-snooping querier vlan 2
Vlan 2:   IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 192.168.12.100
other querier timer            : 120
operational state              : Active
```

- You can use the **run show igmp-snooping mrouter** command to show the information about IGMP snooping router port.

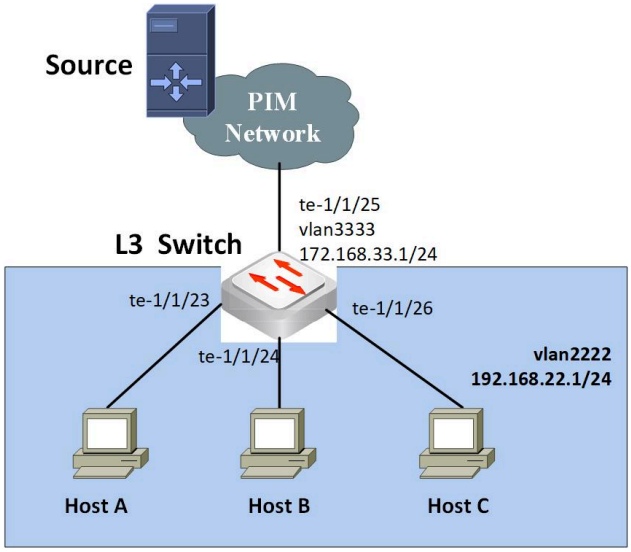
```
admin@XorPlus# run show igmp-snooping mrouter
Vlan      Ports            Type
--------    -------------     ---------
1         ge-1/1/3         Static
```

Example for Configuring IGMP Snooping with IGMP

- Networking Requirements
- Procedure
- Verify Configuration

Networking Requirements

Figure 1. Example for Configuring IGMP Snooping with IGMP



As shown in Figure 1, there are three hosts, Host A, Host B and Host C, in the same network segment, which are multicast receivers. They are connected to the multicast source through the L3 switch and PIM network. The multicast source sends data to the multicast group 224.1.1.1.

In this scenario, the necessary requirement needed to be satisfied is that multicast traffic from the source is forwarded only to the member ports that have sent the IGMP Report messages.

For example, in above figure, assuming that only Host A has sent IGMP Report messages to join the multicast group or replied to a query message, the multicast traffic sent from the source device is expected to be forwarded only to port te-1/1/23, instead of being flooded to all ports of the same VLAN.

To achieve above network requirement, complete the following configurations on the Layer 3 Switch:

- Enable PIM on all the VLAN interfaces (vlan2222 and vlan3333), configure IGMP on host-side VLAN interface (vlan2222).
- Enable IGMP snooping on host VLAN (VLAN ID: 2222).

IGMP snooping establishes and maintains a Layer 2 multicast forwarding table to guide multicast data to be forwarded on demand at the data link layer. By configuring IGMP snooping on the switch, multicast data will not be broadcast at Layer 2, but will be sent to the concerned receiver by the switch.

Procedure

Step1 Configure VLAN and VLAN interface.

```
admin@XorPlus# set vlans vlan-id 2222
admin@XorPlus# set vlans vlan-id 3333
admin@XorPlus# set interface gigabit-ethernet te-1/1/23 family ethernet-switching native-vlan-id 2222
admin@XorPlus# set interface gigabit-ethernet te-1/1/24 family ethernet-switching native-vlan-id 2222
admin@XorPlus# set interface gigabit-ethernet te-1/1/25 family ethernet-switching native-vlan-id 3333
admin@XorPlus# set interface gigabit-ethernet te-1/1/26 family ethernet-switching native-vlan-id 2222
admin@XorPlus# set vlans vlan-id 2222 l3-interface vlan2222
admin@XorPlus# set vlans vlan-id 3333 l3-interface vlan3333
admin@XorPlus# set l3-interface vlan-interface vlan3333 address 172.168.33.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan2222 address 192.168.22.1 prefix-length 24
```

Step2 Enable IP routing.

```
admin@XorPlus# set ip routing enable true
```

Step3 Enable PIM on all the VLAN interfaces, configure IGMP on host-side VLAN interface.

```
admin@XorPlus# set protocols pim interface vlan3333
admin@XorPlus# set protocols pim interface vlan2222
admin@XorPlus# set protocols igmp interface vlan2222 version 3
```

Step4 Enable IGMP snooping on host VLAN.

```
admin@XorPlus# set protocols igmp-snooping enable true
admin@XorPlus# set protocols igmp-snooping vlan-id 2222 enable true
```

Step5 Commit the configurations.

```
admin@XorPlus# commit
```

Verify Configuration

- Run the command **run show igmp groups** to show information about multicast groups and member ports.

```
admin@XorPlus# run show igmp groups
Total IGMP groups: 1
Watermark warn limit(Not Set): 0
Interface        Address         Group           Mode Timer    Srcs V Uptime
vlan2222         192.168.22.1    224.1.1.1       INCL --:--:--    1 3 00:03:01
```

- Run the command **run show mroute** to show the PIM routing table information.

```
admin@XorPlus# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - SGRpt Pruned, F - Register flag, T - SPT-bit set

Source             Group          Flags     Proto    Input            Output           TTL  Uptime
172.168.33.100     224.1.1.1      SCFT      PIM      vlan3333         pimreg           1    00:09:45
                                             IGMP     vlan2222                          1
```

- You can use the **run show igmp-snooping groups** command to show information about the Layer 2 multicast forwarding table.

```
admin@XorPlus# run show igmp-snooping groups
Total group count: 1
Vlan      Group               Port List          Type
--------  ------------------  -----------------  --------------
2222      224.1.1.1           te-1/1/23          Dynamic
```

RFC List

The following table lists the RFC documents related to IGMP snooping.

RFC	Description
RFC4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC1112	Host Extensions for IP Multicasting
RFC2236	Internet Group Management Protocol, Version 2
RFC3376	Internet Group Management Protocol, Version 3

Multicast Source Discovery Protocol (MSDP)

- Introduction of MSDP
- Example for Configuring PIM-SM Inter-domain Multicast Using MSDP
- Example for Configuring Anycast RP
- RFC Lists of MSDP

Introduction of MSDP

Multicast Source Discovery Protocol (MSDP) establishes MSDP peers between routers (usually on RP) in different PIM-SM domains. MSDP peers interchange SA (Source-Active) messages and share multicast source information. Finally, multicast users in one domain can receive multicast data sent by multicast sources in other domains.

Anycast RP is the application of MSDP in a PIM-SM domain. Anycast RP sets up two or more RPs with the same IPv4 address on loopback interfaces in one PIM-SM domain, and establishes MSDP peer relationship between these RPs to achieve load sharing and redundancy backup among the RPs in the domain.

To establish MSDP peers, use the following command lines to configure the MSDP source and member.

set protocols msdp mesh-group < *mesh-group-name*> **member** <*peer-address*>

set protocols msdp mesh-group < *mesh-group-name*> **source** <*source-address*>

Only one mesh group is allowed in a single PIM-SM domain.

When configuring MSDP peers, configure the local MSDP device as the source and all the other remote MSDP peer devices in the same mesh group as the members.

For Anycast RP, MSDP source and member should be configured on the loopback interface.

> **NOTE:**
> MSDP applies only to IPv4 networks.

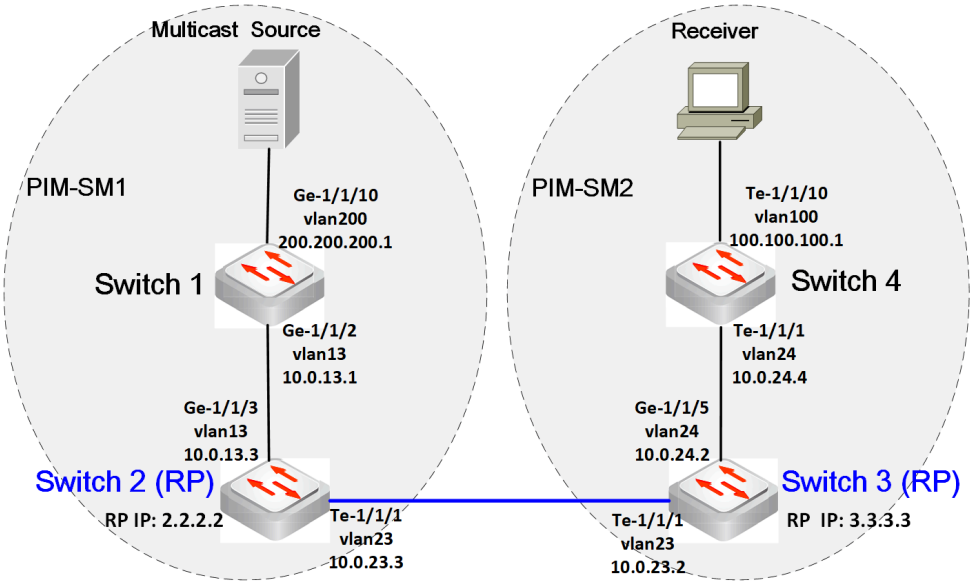
Example for Configuring PIM-SM Inter-domain Multicast Using MSDP

- Network Requirement
  - Figure 1 Network Diagram for Configuring PIM-SM Inter-domain Multicast Using MSDP
- Procedure
  - Switch 1
  - Switch 2
  - Switch 3
  - Switch 4
- Verify the Configuration

Network Requirement

As shown in **Figure 1**, there are two autonomous systems in the network. Each AS contains a PIM-SM domain, the multicast source is in PIM-SM1, the receiver is in PIM-SM2. The network requirement is that the receiver in domain PIM-SM2 can receive multicast data sent by the multicast source in domain PIM-SM1.

Figure 1 Network Diagram for Configuring PIM-SM Inter-domain Multicast Using MSDP



Configuration Roadmap

Configuring MSDP to establish MSDP peer relationship between RPs in each PIM-SM domain to achieve inter-domain multicast communication.

1. Configure the IP address for each switch interface and configure OSPF protocol in the ASs to ensure route reachability within each AS.
2. To ensure route reachability between ASs, configure eBGP peers between ASs and import OSPF routes into BGP.
3. Enable PIM-SM on each multicast interface, and enable IGMP on the host-side interface.
4. Configure static RP on each PIM-SM router in domains PIM-SM1 and PIM-SM2, and specify the loopback interface address of Switch 2 and Switch 3 as the RP address.
5. Configure MSDP source and member on each RP to establish MSDP peer relationship between RPs in each domain.

Procedure

Switch 1

```
admin@Switch1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@Switch1# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching native-vlan-id 200
admin@Switch1# set ip routing enable true
admin@Switch1# set l3-interface vlan-interface vlan200 address 200.200.200.1 prefix-length 24
admin@Switch1# set l3-interface vlan-interface vlan13 address 10.0.13.1 prefix-length 24
admin@Switch1# set protocols ospf router-id 1.1.1.1
admin@Switch1# set protocols ospf network 200.200.200.0/24 area 0
admin@Switch1# set protocols ospf network 10.0.13.0/24 area 0
admin@Switch1# set protocols pim rp 3.3.3.3 group 224.0.0.0/4
admin@Switch1# set protocols pim interface vlan200
admin@Switch1# set protocols pim interface vlan13
admin@Switch1# set vlans vlan-id 13 l3-interface vlan13
admin@Switch1# set vlans vlan-id 200 l3-interface vlan200
```

```
admin@Switch1# commit
```

Switch 2

```
admin@Switch2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 13
admin@Switch2# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 23
admin@Switch2# set ip routing enable true
admin@Switch2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@Switch2# set l3-interface vlan-interface vlan13 address 10.0.13.3 prefix-length 24
admin@Switch2# set l3-interface vlan-interface vlan23 address 10.0.23.3 prefix-length 24
admin@Switch2# set protocols bgp local-as 100
admin@Switch2# set protocols bgp router-id 2.2.2.2
admin@Switch2# set protocols bgp neighbor 10.0.23.2 remote-as 200
admin@Switch2# set protocols bgp ipv4-unicast redistribute connected
admin@Switch2# set protocols bgp ipv4-unicast redistribute ospf
admin@Switch2# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Switch2# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Switch2# set protocols ospf router-id 2.2.2.2
admin@Switch2# set protocols ospf network 2.2.2.2/32 area 0
admin@Switch2# set protocols ospf network 10.0.13.0/24 area 0
admin@Switch2# set protocols ospf redistribute bgp
admin@Switch2# set protocols pim rp 3.3.3.3 group 224.0.0.0/4
admin@Switch2# set protocols pim interface lo
admin@Switch2# set protocols pim interface vlan13
admin@Switch2# set protocols pim interface vlan23
admin@Switch2# set vlans vlan-id 13 l3-interface vlan13
admin@Switch2# set vlans vlan-id 23 l3-interface vlan23
admin@Switch2# commit
```

Switch 3

```
admin@Switch3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 24
admin@Switch3# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 23
admin@Switch3# set ip routing enable true
admin@Switch3# set l3-interface loopback lo address 3.3.3.3 prefix-length 32
admin@Switch3# set l3-interface vlan-interface vlan24 address 10.0.24.2 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan23 address 10.0.23.2 prefix-length 24
admin@Switch3# set protocols bgp local-as 200
admin@Switch3# set protocols bgp router-id 3.3.3.3
admin@Switch3# set protocols bgp neighbor 10.0.23.3 remote-as 100
admin@Switch3# set protocols bgp ipv4-unicast redistribute connected
admin@Switch3# set protocols bgp ipv4-unicast redistribute ospf
admin@Switch3# set protocols msdp mesh-group 6.6.6.6 member 2.2.2.2
admin@Switch3# set protocols msdp mesh-group 6.6.6.6 source 3.3.3.3
admin@Switch3# set protocols ospf router-id 3.3.3.3
admin@Switch3# set protocols ospf network 10.0.24.0/24 area 0
admin@Switch3# set protocols ospf network 3.3.3.3/32 area 0
admin@Switch3# set protocols ospf redistribute bgp
admin@Switch3# set protocols pim rp 2.2.2.2 group 224.0.0.0/4
admin@Switch3# set protocols pim interface vlan24
admin@Switch3# set protocols pim interface lo
admin@Switch3# set protocols pim interface vlan23
admin@Switch3# set vlans vlan-id 23 l3-interface vlan23
admin@Switch3# set vlans vlan-id 24 l3-interface vlan24
admin@Switch3# commit
```

Switch 4

```
admin@Switch4# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 24
admin@Switch4# set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 100
admin@Switch4# set ip routing enable true
admin@Switch4# set l3-interface vlan-interface vlan24 address 10.0.24.4 prefix-length 24
admin@Switch4# set l3-interface vlan-interface vlan100 address 100.100.100.1 prefix-length 24
admin@Switch4# set protocols igmp interface vlan100
admin@Switch4# set protocols ospf router-id 4.4.4.4
```

```
admin@Switch4# set protocols ospf network 10.0.24.0/24 area 0
admin@Switch4# set protocols ospf network 100.100.100.0/24 area 0
admin@Switch4# set protocols pim rp 2.2.2.2 group 224.0.0.0/4
admin@Switch4# set protocols pim interface vlan24
admin@Switch4# set protocols pim interface vlan100
admin@Switch4# set vlans vlan-id 24 l3-interface vlan24
admin@Switch4# set vlans vlan-id 100 l3-interface vlan100
admin@Switch4# commit
```

Verify the Configuration

- You can view the establishment state for MSDP peers by using the **run show msdp mesh-group** command.

```
admin@Switch2# run show msdp mesh-group
Mesh group : 6.6.6.6
  Source : 2.2.2.2
  Member                State
  3.3.3.3          established

admin@Switch3# run show msdp mesh-group
Mesh group : 6.6.6.6
  Source : 3.3.3.3
  Member                State
  2.2.2.2          established
```

- You can view PIM routes on the switches by using **run show mroute** Multicast source 200.200.200.2 in the PIM-SM1 domain sends multicast data to multicast groups 237.0.0.1, 237.0.0.2, 237.0.0.3, 237.0.0.4, 237.0.0.5, 238.0.0.1 and 239.255.255.250. Receiver in PIM-SM2 can receive the multicast data.

```
admin@Switch2# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group           Flags           Proto  Input           Output          TTL  Uptime
200.200.200.2   237.0.0.1       ST              PIM    vlan13          vlan23          1    00:16:30
200.200.200.2   237.0.0.2       ST              PIM    vlan13          vlan23          1    00:15:56
200.200.200.2   237.0.0.3       ST              PIM    vlan13          vlan23          1    00:15:56
200.200.200.2   237.0.0.4       ST              PIM    vlan13          vlan23          1    00:15:56
200.200.200.2   237.0.0.5       ST              PIM    vlan13          vlan23          1    00:15:56
200.200.200.2   238.0.0.1       ST              PIM    vlan13          vlan23          1    00:16:30
200.200.200.2   239.255.255.250 ST              PIM    vlan13          vlan23          1    00:16:30

admin@Switch3# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group          Flags            Proto  Input           Output          TTL  Uptime
*               237.0.0.1       S               PIM    lo              vlan24          1    00:40:32
200.200.200.2   237.0.0.1       ST              PIM    vlan23          vlan24          1    00:41:02
*               237.0.0.2       S               PIM    lo              vlan24          1    00:40:35
200.200.200.2   237.0.0.2       ST              PIM    vlan23          vlan24          1    00:41:02
*               237.0.0.3       S               PIM    lo              vlan24          1    00:40:30
200.200.200.2   237.0.0.3       ST              PIM    vlan23          vlan24          1    00:41:02
*               237.0.0.4       S               PIM    lo              vlan24          1    00:40:31
200.200.200.2   237.0.0.4       ST              PIM    vlan23          vlan24          1    00:41:02
*               237.0.0.5       S               PIM    lo              vlan24          1    00:40:27
200.200.200.2   237.0.0.5       ST              PIM    vlan23          vlan24          1    00:41:02
*               238.0.0.1       S               PIM    lo              vlan24          1    00:40:28
200.200.200.2   238.0.0.1       ST              PIM    vlan23          vlan24          1    00:41:02
*               239.255.255.250 S               PIM    lo              vlan24          1    00:40:27
200.200.200.2   239.255.255.250 ST              STAR   vlan23          vlan24          1    00:41:02
```

- You can view (S, G) entries cache on MSDP peer switches by using the **run show msdp sa** "**RP**" is the source RP address that advertises the (S, G) entry. "**RP**" value "-" indicates that the device running the show command is the source RP advertising the (S, G) entry.

```
admin@Switch3# run show msdp sa
Source                 Group                 RP  Local  SPT    Uptime
200.200.200.2         237.0.0.1              -      y    -  00:01:39
```

```
200.200.200.2          237.0.0.2               -      y    -  00:00:06
200.200.200.2          237.0.0.3               -      y    -  00:00:06
200.200.200.2          237.0.0.4               -      y    -  00:00:06
200.200.200.2          237.0.0.5               -      y    -  00:00:06
200.200.200.2          238.0.0.1               -      y    -  00:01:39

admin@Switch2# run show msdp sa
Source                  Group            RP      Local  SPT  Uptime
200.200.200.2          237.0.0.1         3.3.3.3      n    y  00:32:16
200.200.200.2          237.0.0.2         3.3.3.3      n    y  00:00:39
200.200.200.2          237.0.0.3         3.3.3.3      n    y  00:00:39
200.200.200.2          237.0.0.4         3.3.3.3      n    y  00:00:39
200.200.200.2          237.0.0.5         3.3.3.3      n    y  00:00:39
200.200.200.2          238.0.0.1         3.3.3.3      n    y  00:32:16
200.200.200.2    239.255.255.250         3.3.3.3      n    y  00:00:11
```

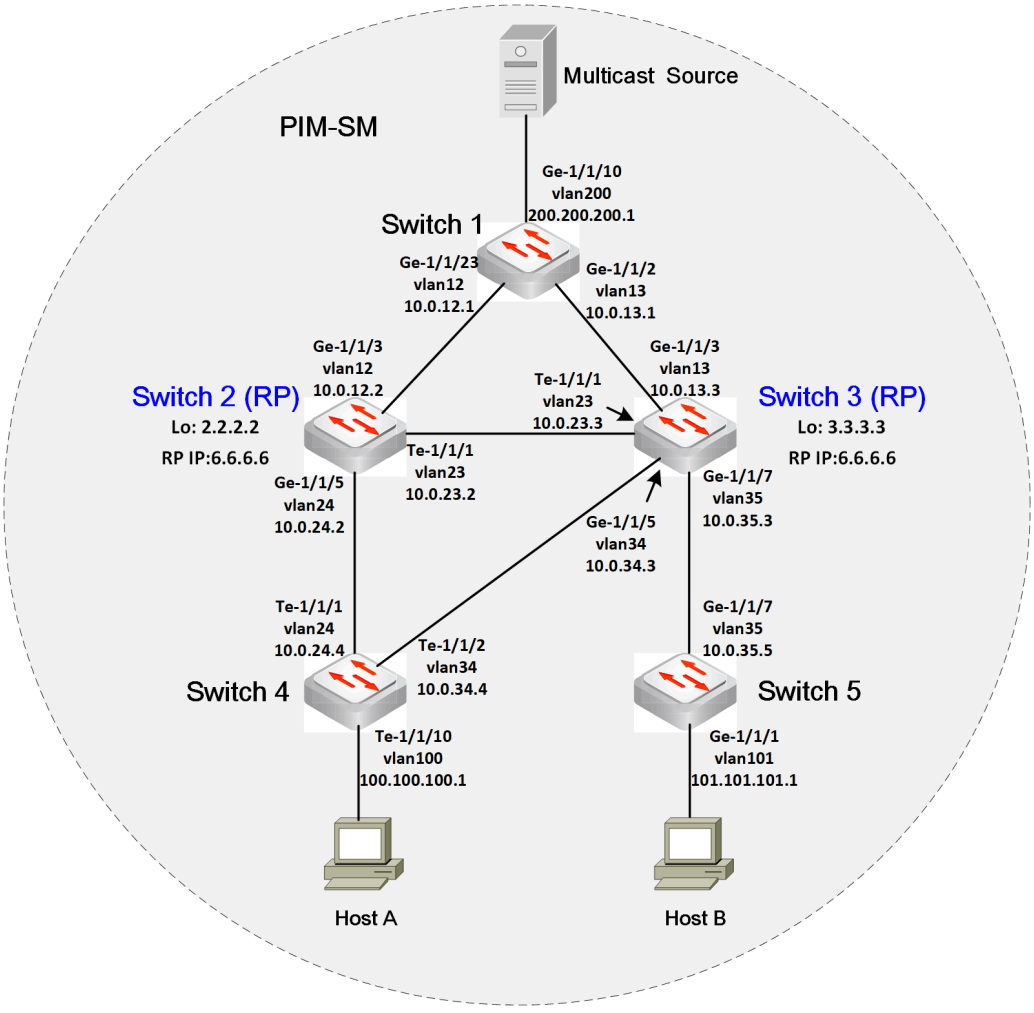
Example for Configuring Anycast RP

- Network Requirement
  - Figure 1 Network Diagram for Configuring Anycast RP
- Procedure
  - Switch 1
  - Switch 2
  - Switch 3
  - Switch 4
  - Switch 5
- Verify the Configuration

Network Requirement

As shown in **Figure 1**, in the PIM-SM domain, the multicast source sends multicast data to group 238.0.0.1, and Host A and Host B are members of this multicast group.

Figure 1 Network Diagram for Configuring Anycast RP



Apply Anycast RP in the PIM-SM domain to achieve load sharing and backup among multiple RPs.

1. Select Switch 2 and Switch 3 as the anycast RPs in the PIM-SM domain.
2. Prepare a loopback interface address respectively on Switch 2 and Switch 3 with the same value.
3. Configure the RP. Configure static RP on each PIM-SM router in the whole domain, specifying the loopback interface address of Switch 2 and Switch 3 as the RP address.
4. Prepare another loopback interface address on Switch 2 and Switch 3 respectively, which will be used to establish MSDP peer connection. Do not use the loopback interface address used for the RP.
5. Use the following command lines to establish the MSDP peer connection between Switch 2 and Switch 3.

set protocols msdp mesh-group < *mesh-group-name*> **member** <*peer-address*>

set protocols msdp mesh-group < *mesh-group-name*> **source** <*source-address*>

Procedure

Switch 1

```
admin@Switch1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 13
admin@Switch1# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching native-vlan-id 200
admin@Switch1# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 12
admin@Switch1# set ip routing enable true
admin@Switch1# set l3-interface vlan-interface vlan12 address 10.0.12.1 prefix-length 24
admin@Switch1# set l3-interface vlan-interface vlan200 address 200.200.200.1 prefix-length 24
admin@Switch1# set l3-interface vlan-interface vlan13 address 10.0.13.1 prefix-length 24
admin@Switch1# set protocols ospf router-id 1.1.1.1
admin@Switch1# set protocols ospf network 10.0.12.0/24 area 0.0.0.0
admin@Switch1# set protocols ospf network 200.200.200.0/24 area 0
admin@Switch1# set protocols ospf network 10.0.13.0/24 area 0
admin@Switch1# set protocols ospf interface vlan13 cost 15
admin@Switch1# set protocols pim rp 6.6.6.6 group 224.0.0.0/4
admin@Switch1# set protocols pim interface vlan12
admin@Switch1# set protocols pim interface vlan200
admin@Switch1# set protocols pim interface vlan13
admin@Switch1# set vlans vlan-id 12 l3-interface vlan12
admin@Switch1# set vlans vlan-id 13 l3-interface vlan13
admin@Switch1# set vlans vlan-id 200 l3-interface vlan200
admin@Switch1# commit
```

Switch 2

```
admin@Switch2# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 12
admin@Switch2# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 24
admin@Switch2# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 23
admin@Switch2# set ip routing enable true
admin@Switch2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@Switch2# set l3-interface loopback lo address 6.6.6.6 prefix-length 32
admin@Switch2# set l3-interface vlan-interface vlan24 address 10.0.24.2 prefix-length 24
admin@Switch2# set l3-interface vlan-interface vlan12 address 10.0.12.2 prefix-length 24
admin@Switch2# set l3-interface vlan-interface vlan23 address 10.0.23.2 prefix-length 24
admin@Switch2# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Switch2# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Switch2# set protocols spanning-tree enable false
admin@Switch2# set protocols ospf router-id 2.2.2.2
admin@Switch2# set protocols ospf network 10.0.12.0/24 area 0
admin@Switch2# set protocols ospf network 10.0.24.0/24 area 0
admin@Switch2# set protocols ospf network 2.2.2.2/32 area 0
admin@Switch2# set protocols ospf network 10.0.23.0/24 area 0
admin@Switch2# set protocols ospf network 6.6.6.6/32 area 0
admin@Switch2# set protocols pim rp 6.6.6.6 group 224.0.0.0/4
admin@Switch2# set protocols pim interface vlan12
admin@Switch2# set protocols pim interface vlan24
admin@Switch2# set protocols pim interface lo
admin@Switch2# set protocols pim interface vlan23
admin@Switch2# set vlans vlan-id 12 l3-interface vlan12
admin@Switch2# set vlans vlan-id 23 l3-interface vlan23
admin@Switch2# set vlans vlan-id 24 l3-interface vlan24
admin@Switch2# commit
```

Switch 3

```
admin@Switch3# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 13
admin@Switch3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 34
admin@Switch3# set interface gigabit-ethernet ge-1/1/7 family ethernet-switching native-vlan-id 35
admin@Switch3# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 23
admin@Switch3# set ip routing enable true
admin@Switch3# set l3-interface loopback lo address 3.3.3.3 prefix-length 32
admin@Switch3# set l3-interface loopback lo address 6.6.6.6 prefix-length 32
admin@Switch3# set l3-interface vlan-interface vlan34 address 10.0.34.3 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan13 address 10.0.13.3 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan23 address 10.0.23.3 prefix-length 24
```

```
admin@Switch3# set l3-interface vlan-interface vlan35 address 10.0.35.3 prefix-length 24
admin@Switch3# set protocols msdp mesh-group 6.6.6.6 member 2.2.2.2
admin@Switch3# set protocols msdp mesh-group 6.6.6.6 source 3.3.3.3
admin@Switch3# set protocols ospf router-id 3.3.3.3
admin@Switch3# set protocols ospf network 10.0.34.0/24 area 0.0.0.0
admin@Switch3# set protocols ospf network 6.6.6.6/32 area 0
admin@Switch3# set protocols ospf network 3.3.3.3/32 area 0
admin@Switch3# set protocols ospf network 10.0.13.0/24 area 0
admin@Switch3# set protocols ospf network 10.0.23.0/24 area 0
admin@Switch3# set protocols ospf network 10.0.35.0/24 area 0
admin@Switch3# set protocols pim rp 6.6.6.6 group 224.0.0.0/4
admin@Switch3# set protocols pim interface vlan34
admin@Switch3# set protocols pim interface lo
admin@Switch3# set protocols pim interface vlan13
admin@Switch3# set protocols pim interface vlan23
admin@Switch3# set protocols pim interface vlan35
admin@Switch3# set vlans vlan-id 13 l3-interface vlan13
admin@Switch3# set vlans vlan-id 23 l3-interface vlan23
admin@Switch3# set vlans vlan-id 34 l3-interface vlan34
admin@Switch3# set vlans vlan-id 35 l3-interface vlan35
admin@Switch3# commit
```

Switch 4

```
admin@Switch4# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 24
admin@Switch4# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 34
admin@Switch4# set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 100
admin@Switch4# set ip routing enable true
admin@Switch4# set l3-interface vlan-interface vlan24 address 10.0.24.4 prefix-length 24
admin@Switch4# set l3-interface vlan-interface vlan34 address 10.0.34.4 prefix-length 24
admin@Switch4# set l3-interface vlan-interface vlan100 address 100.100.100.1 prefix-length 24
admin@Switch4# set protocols igmp interface vlan100
admin@Switch4# set protocols ospf router-id 4.4.4.4
admin@Switch4# set protocols ospf network 10.0.24.0/24 area 0
admin@Switch4# set protocols ospf network 10.0.34.0/24 area 0
admin@Switch4# set protocols ospf network 100.100.100.0/24 area 0
admin@Switch4# set protocols ospf interface vlan34 cost 15
admin@Switch4# set protocols pim rp 6.6.6.6 group 224.0.0.0/4
admin@Switch4# set protocols pim interface vlan24
admin@Switch4# set protocols pim interface vlan34
admin@Switch4# set protocols pim interface vlan100
admin@Switch4# set vlans vlan-id 24 l3-interface vlan24
admin@Switch4# set vlans vlan-id 34 l3-interface vlan34
admin@Switch4# set vlans vlan-id 100 l3-interface vlan100
admin@Switch4# commit
```

Switch 5

```
admin@Switch5# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 101
admin@Switch5# set interface gigabit-ethernet ge-1/1/7 family ethernet-switching native-vlan-id 35
admin@Switch5# set l3-interface vlan-interface vlan35 address 10.0.35.5 prefix-length 24
admin@Switch5# set l3-interface vlan-interface vlan101 address 101.101.101.1 prefix-length 24
admin@Switch5# set protocols igmp interface vlan101
admin@Switch5# set protocols ospf router-id 5.5.5.5
admin@Switch5# set protocols ospf network 10.0.35.0/24 area 0
admin@Switch5# set protocols pim rp 6.6.6.6 group 224.0.0.0/4
admin@Switch5# set protocols pim interface vlan35
admin@Switch5# set protocols pim interface vlan101
admin@Switch5# set vlans vlan-id 35 l3-interface vlan35
admin@Switch5# set vlans vlan-id 101 l3-interface vlan101
admin@Switch5# commit
```

Verify the Configuration

- You can use command **run show msdp mesh-group** to check the establishment state for MSDP peers.

```
admin@Switch2# run show msdp mesh-group
Mesh group : 6.6.6.6
  Source : 2.2.2.2
  Member         State
  3.3.3.3          established
```

- You can use command **run show msdp peer** command to view the detail information about the remote MSDP peer.

```
admin@Switch2# run show msdp peer detail
Peer : 3.3.3.3
  Local               : 2.2.2.2
  Mesh Group          : 6.6.6.6
  State               : established
  Uptime              : 06:10:52
  Keepalive Timer     : 00:00:08
  Conn Retry Timer    : --:--:--
  Hold Timer          : 00:00:46
  Last Reset          : -
  Conn Attempts       : 22
  Established Changes : 1
  SA Count            : 2
  Statistics          :
                       Sent       Rcvd
    Keepalives :        371          4
  SAs        :          0        748
```

- You can view PIM routes on the switches by using the **run show mroute** Multicast source 200.200.200.2 in the PIM-SM domain sends multicast data to multicast group 238.0.0.1, and Host A joins multicast group 238.0.0.1 to receive multicast data sent to group 238.0.0.1.

By comparing the PIM routes on Switch 2, Switch 3 and Switch 4, we can see that the current valid RP is Switch 2: the multicast source registers with Switch 2 and Host A joins Switch 2. No PIM routes are displayed on Switch 3.

```
admin@Switch2# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group          Flags   Proto   Input            Output          TTL  Uptime
*               238.0.0.1       S       PIM    lo               vlan24          1    00:04:35
200.200.200.2   238.0.0.1       ST      STAR   vlan12           vlan24          1    00:04:37

admin@Switch3# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group           Flags   Proto  Input            Output          TTL  Uptime


admin@Switch4# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group          Flags   Proto   Input            Output          TTL  Uptime
*               238.0.0.1       SC     IGMP   vlan24          vlan100          1    02:00:31
```

- You can view the RP information by using the **run show pim rp-info** command.

```
admin@Switch2# run show pim rp-info
RP address       group/prefix-list   OIF              I am RP    Source
6.6.6.6          224.0.0.0/4         lo               yes        Static

admin@Switch3#run show pim rp-info
RP address       group/prefix-list   OIF              I am RP    Source
6.6.6.6          224.0.0.0/4         lo               yes        Static

admin@Switch4#run show pim rp-info
RP address       group/prefix-list   OIF              I am RP    Source
```

```
6.6.6.6          224.0.0.0/4         vlan24            no        Static
```

RFC Lists of MSDP

The development of PICOS MSDP and anycast RP are based on FRR and implemented according to IETF standard protocols described in RFC 3618 and RFC 3446.

RFC	Description
RFC 3618	Multicast Source Discovery Protocol (MSDP)
RFC 3446	Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

Multicast VLAN Registration (MVR)

- Overview of MVR
- Configuration Notes and Constraints of MVR
- Configuring MVR

Overview of MVR

- Overview
- Terminology
- MVR Operation Mechanism

Overview

Multicast VLAN Registration (MVR) is designed for different end user devices, such as IPTVs to receive the same source multicast traffic across the Ethernet network with different service VLAN tags. Usually, different end users are isolated with different service VLAN ID for security reason. Multicast stream from the upstream port is forwarded to multi-access ports tagged with different service VLAN ID.

On the other hand, the IGMP report packets from access ports for joining or leaving the multicast group, are tagged with different service VLAN IDs. When forwarding the IGMP packets to multicast router, the VLAN ID of the packets should be changed to upstream VLAN ID so as to talk to IGMP router.

Terminology

MVR

Multicast VLAN Registration is designed for delivering IPTV multicast streams over ethernet network from the same source, group and VLAN ID to different receivers in different VLAN. The VLAN ID translation should be done for the multicast traffic data and IGMP control packets between the upstream port and access ports.

MVR VLAN

It is the VLAN ID of the multicast traffic from the upstream ports connected to the multicast router. The IGMP control packets from the multicast router also use the same VLAN ID to talk to any receiver devices.

Receiver VLAN

It is the service VLAN ID allocated for one end user/device, which is connected to access port of the switch for receiving the multicast traffic.

Mrouter Port

Mrouter port is the upstream port of the switch that is connected to the multicast router for delivering the multicast traffic to end users.

IGMP Snooping

IGMP Snooping listens to IGMP packets between router and access ports of the interested multicast groups, so as to do L2 forwarding accordingly without flooding.

IGMP Packet

IGMP packet is the control message packets between IGMP router and receiver devices for joining or leaving the multicast stream.

MVR Operation Mechanism

MVR does the VLAN translation of multicast traffic on both directions from mrouter to user access port, and from access to mrouter port. There are two types of packets, multicast IGMP control packets and multicast data packets.

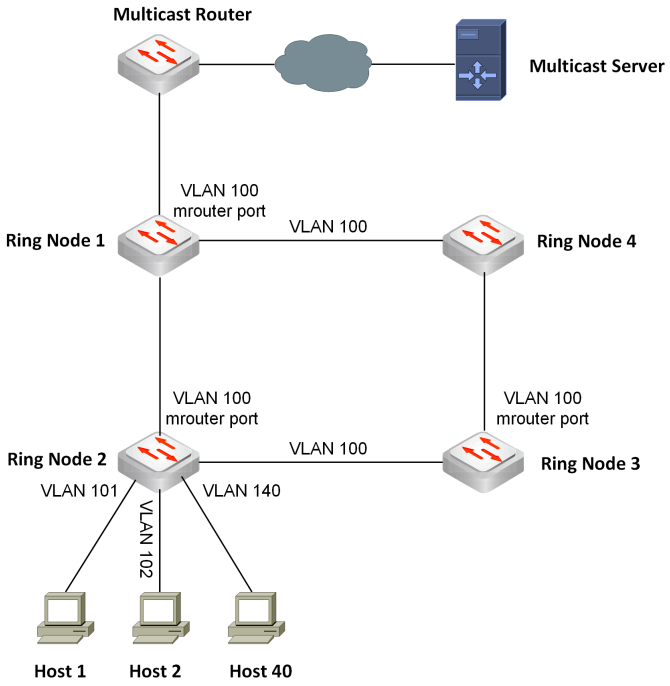
The multicast protocol control packets from upstream router, such as IGMP Query packets from mrouter port will be intercepted and sent out to all ports in the mapped VLAN list of the corresponding multicast group. On the other hand, the IGMP multicast group join/leave packets from receiver devices will be intercepted and translated to MVR VLAN and sent out from the mrouter port. The upstream multicast router doesn't feel any difference if the MVR is enabled or not on the switch side.

The multicast data traffic from upstream ports will be translated to the receiver VLAN ID accordingly based on IGMP Snooping messages from each access port.

On the other hand, the multicast traffic will be forwarded to the trunk ports with same VLAN ID as the MVR VLAN.

For example, in **Figure 1** sample MVR topology, the multicast router will send IGMP Query packets to Ring Node 1. If RPL link of the ERPS instance VLAN 100 is between Node 1 and Node 4, the IGMP Query packets will be forwarded to Node 2. Node 2 will forward the Query to Host 1 to Host 40, and another ERPS port1 to Node 3, and node 3 to Node 4 as well.

Figure 1. Sample MVR Topology



On ERPS Node 3, the IGMP Query packets will be forwarded to all access ports in the VLAN list with VLAN changed accordingly. When the host sends back the IGMP report packets, the VLAN will be modified to MVR VLAN and sent out from upstream port0 to multicast router.

The multicast data traffic from Node 1 will be forwarded out to Node 3 through ERPS port1 without changing of the data VLAN.

Configuration Notes and Constraints of MVR

When configure the MVR, please pay attention to the following notes:

- Static MVR configuration is not supported in current MVR version.
- PICOS supports a maximum of 255 multicast groups in IGMP snooping forwarding table for MVR.
- The IGMP snooping is by default automatically enabled for all receiver VLAN IDs.
- Group overlapping is not allowed when configuring multiple MVLANs.
- One receiver VLAN can only be mapped to one MVLAN on one interface.
- The multicast traffic will be forwarded to the trunk ports which have the same VLAN ID as MVLAN.
- The MVLAN and its binding receiver VLANs should be in the same spanning tree instance.

Configuring MVR

- Configuring MVR
- Configuration Example
  - Networking Requirements
  - Procedure
  - Verifying the Configuration

Configuring MVR

Step1 Configure VLANs for upstream port and access port respectively.

set interface gigabit-ethernet *<interface-name>* **family ethernet-switching port-mode** *<port-mode>*

set interface gigabit-ethernet *<interface-name>* **family ethernet-switching vlan members** *<vlan-id>*

Step2 Enable IGMP snooping globally.

set protocols igmp-snooping enable true

Step3 Configure mrouter port.

set protocols igmp-snooping vlan-id *<vlan-id>* **mrouter interface** *<interface-name>*

Step4 Configure MVR source group.

set protocols igmp-snooping vlan-id *<vlan-id>* **mvr source group** *<multicast-network-address>/<prefix-length>*

Step5 Configure receiver VLAN list.

set protocols igmp-snooping vlan-id *<vlan-id>* **mvr receiver vlan-list** *<vlan range string>*

Step6 Commit the configuration.

commit

Step7 View the configuration information of MVR.

run show igmp-snooping mvr mvlan *<vlan-id>*

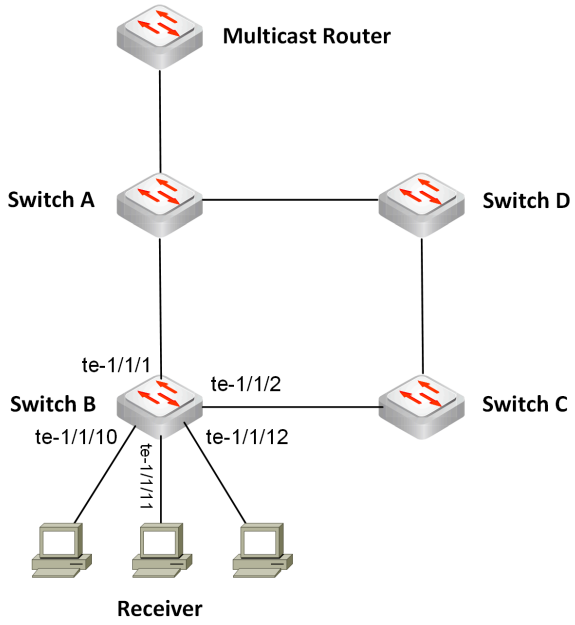
run show igmp-snooping mvr receiver-vlan *<vlan-id>*

Configuration Example

Networking Requirements

Switch B is one node of the ERPS ring, of which VLAN 100 is the ring instance member (Please refer to ERPS section for how to configure the ERPS ring and instance). The two ports, te-1/1/1/1 and te-1/1/2 are ring port0 and port1, both are mrouter ports as well.

Figure 1. MVR Configuration Example



Port te-1/1/10, te-1/1/11 and te-1/1/12 are the access ports with VLAN ID as 101, 102 and 103 respectively.

Procedure

Switch B

Step1 Enable IGMP snooping globally.

```
admin@SwitchB# set protocols igmp-snooping enable true
```

Step2 Configure upstream mrouter ports.

```
admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@SwitchB# set protocols igmp-snooping vlan-id 100 mrouter interface te-1/1/1
admin@SwitchB# set protocols igmp-snooping vlan-id 100 mrouter interface te-1/1/2
```

Step3 Configure MVLAN and source groups.

```
admin@SwitchB# set protocols igmp-snooping vlan-id 100 mvr source group 225.0.0.1/32
```

Step4 Configure access ports.

```
admin@SwitchB# set interface gigabit-ethernet te-1/1/10 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/10 family ethernet-switching vlan members 101
admin@SwitchB# set interface gigabit-ethernet te-1/1/11 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/11 family ethernet-switching vlan members 102
admin@SwitchB# set interface gigabit-ethernet te-1/1/12 family ethernet-switching port-mode trunk
admin@SwitchB# set interface gigabit-ethernet te-1/1/12 family ethernet-switching vlan members 103
```

Step5 Configure MVR receiver VLAN IDs.

```
admin@SwitchB# set protocols igmp-snooping vlan-id 100 mvr receiver vlan-list 101-103
```

Step6 Commit the configurations.

```
admin@SwitchB# commit
```

Verifying the Configuration

- The command **run show igmp-snooping mvr mvlan** <*vlan-id*> can be used to check the MVLAN(s) of the MVR.

```
admin@SwitchB# run show igmp-snooping mvr mvlan 100
Mvlan      Receiver-vlan
--------  ------------------
100       101, 102, 103
```

- The command **run show igmp-snooping mvr receiver-vlan** <*vlan-id*> will show the receiver VLAN and MVR VLAN information.

```
admin@SwitchB# run show igmp-snooping mvr receiver-vlan 101
Receiver-vlan   Mvlan
-------------  ----------
101             100
```

- You can use the **run show igmp-snooping groups** command to show information about multicast group member ports which is used for Layer 2 forwarding, namely, the Layer 2 forwarding table. **Port List** shows the egress ports for multicast packets.

```
admin@SwitchB# run show igmp-snooping groups
Vlan      Group                 Port List          Type
--------  ------------------    -----------------   ----------------------
100       225.0.0.1              te-1/1/10          Dynamic
                                 te-1/1/11          Dynamic
                                 te-1/1/1           Mrouter
```

ACL Configuration

- Configuring Basic ACL
- Configuring Time Range

Configuring Basic ACL

In L2/L3, ACLs support destination-address-ipv4, destination-address-ipv6, destination-mac-address, destination-port, ether-type, ip, protocol, source-address-ipv4, source-address-ipv6, source-mac-address, source-port, and vlan-id.

TCP flags are also supported. These ACLs can be applied to physical ports, LAG ports, and VLAN interfaces. One ACL can be applied to multiple ports (the properties of the ports can be same or different), but only one port can be matched to one ACL.

- It does not allow to configure different firewall filters to the same VLAN interface on ingress side or egress side.
- ACL can't filter layer 2 protocol packets, for example BPDU, LLDP, LACP and so on.
- Packets with any of the following destination MACs will always be sent to CPU even if ACL policy has been configured to discard the packets.

  01:80:c2:00:00:10
  01:80:c2:00:00:20/ff:ff:ff:ff:ff:f0
  01:80:c2:00:00:00/ff:ff:ff:ff:ff:f0
- Matching field **protocol icmp** of ACL rules on output interface are not supported on all the platforms.
- Matching fields **destination-mac-address**, **ether-type**, **vlan**, **first-fragment**, **ip-fragment** and **source-mac-address** of ACL rules on output interface inbound-control-plane are not supported on all the platforms.
- The match counter statistics information of the ACL filter is cleared when adding a new filter, modifying, or deleting an old filter. When there is a new packet, new match counter statistics information will be generated.
- **set firewall filter sequence from protocol icmp** and **set firewall filter sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter sequence from protocol others** command with the protocol number.
- When matching ACL rules, the system processes IPv6 rules (**destination-address-ipv6/source-address-ipv6**) with higher priority than other ACL rules. Even if the sequence number of IPv6 rule is larger than the other rules', the IPv6 rule will be processed first.
  For example, confider the ACL rules shown below. The **destination-address-ipv6** rule will be processed first then all the other rules will be processed.

  admin@XorPlus# set firewall filter MyFilter sequence 100 from destination-mac-address 44:44:44:44:44:44
  admin@XorPlus# set firewall filter MyFilter sequence 100 then action discard
  admin@XorPlus# set firewall filter MyFilter sequence 200 from destination-address-ipv6 2001::1/128
  admin@XorPlus# set firewall filter MyFilter sequence 200 then action forward

  Therefore, when planning ACL rules, it is recommended to configure IPv6 source/destination rules with smaller sequence numbers. If not then it is highly stressed to keep this exception in mind while trying to achieve the desired effect.
- IPv6 ACL rules cannot be configured with the following rules at the same time:
  - Configuration with ether-type or destination-port is not supported on the ingress port.
  - Configuration with destination-mac-address or source-mac-address or ether-type is not supported on the egress port.
- Please note: There is always an implicit discard action rule at the end of all ACL rules.
- If all the ACL rules specify discard actions only, then add a forward all action rule at the end of the ACL to specify that all "unmatched" packets will be forwarded. Example: set firewall filter bad-net sequence 999 then action forward

Configuring ACLs

```
admin@XorPlus# set firewall filter bad-net sequence 111 from source-address-ipv4 1.1.1.0/24
admin@XorPlus# set firewall filter bad-net sequence 111 then action discard
admin@XorPlus# set firewall filter bad-net sequence 112 from source-address-ipv4 1.1.2.0/24
admin@XorPlus# set firewall filter bad-net sequence 112 then action discard
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set firewall filter bad-net input interface ge-1/1/1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set firewall filter bad-net input interface ae1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

When the switch receives a packet in ingress and egress, it will attempt to match ACLs by sequence number, with smaller values representing higher priorities. If the matched ACL's action is "forward" or "discard," the switch will forward or discard the packet and will not match the remaining ACLs. If there is no matching ACL, the packet will be dropped.

Configuring ACLs in VLANs

Every member port in the VLAN interface will be applied with the ACLs configured in the VLAN interface.

```
admin@XorPlus# set firewall filter bad-net sequence 221 from source-address-ipv4 1.1.1.0/24
```

```
admin@XorPlus# set firewall filter bad-net sequence 221 then action discard
admin@XorPlus# set firewall filter bad-net sequence 222 from source-address-ipv4 1.1.2.0/24
admin@XorPlus# set firewall filter bad-net sequence 222 then action discard
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set vlans vlan-id 2 l3-interface vlan-2
admin@XorPlus# set l3-interface vlan-interface vlan-2
admin@XorPlus# set firewall filter bad-net input vlan-interface vlan-2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring ACL Discard TCP ACK

You can configure ACL TCP flags (ACK/FIN/PSH/RST/SYN/URG/TCP-ESTABLISHED/TCP-INITIAL) to specify what action (forward/discard) to perform on which packets (true/false).

```
admin@XorPlus# set firewall filter bad-net sequence 331 then action discard
admin@XorPlus# set firewall filter bad-net sequence 331 from protocol tcp flags ack true
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set firewall filter bad-net output interface ge-1/1/1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Configuring ACL logging for Match Statistics

```
admin@XorPlus# set firewall filter bad-net sequence 441 then action discard
admin@XorPlus# set firewall filter bad-net sequence 441 from destination-address-ipv4 192.168.100.0/24
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set firewall filter bad-net input interface ge-1/1/1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set firewall filter bad-net sequence 441 log interval 10
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# run syslog monitor on
admin@XorPlus#
```

Check the Configuration

```
admin@XorPlus# run show filter
Filter: bad-net
          Description:
          Sequence: 111
              Description:
              match counter:  0 packets
              match-condition:
                 source-address-ipv4:                1.1.1.0/24
              action: discard
              forwarding_class:
          Sequence: 112
```

```
               Description:
               match counter:  0 packets
               match-condition:
                  source-address-ipv4:                1.1.2.0/24
               action: discard
               forwarding_class:
              Input interface: ge-1/1/1
Filter: copp
          Description:
          Sequence: 10
              Description:
              match counter:  0 packets
              match-condition:
                 protocol:                bpdu
              action: forward
              forwarding_class: bpdu-class
             ......
```

Configuring Time Range

- Overview
- Example for Configuring ACL Rule of Time Range
  - Networking Requirements
  - Procedure
  - Verify Configuration

Overview

Time range is a periodic time period configured on the switch. It's a fixed time period for each week. For example, from 8:00 to 18:00 from Monday to Friday. The system starts this time at a fixed time of the week. Time ranges are used in ACL rules as a filtering condition to restrict the effective time period of an ACL filtering rule, so as to filter traffic flows within a certain time period. For example, restrict users accessing to a server at a specific time period. The system starts the time at a fixed time of the week according to the system clock after applied the time range to the ACL rules.

Users can use the following two command to configure a pair of starting time and ending time to define a time range.

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **start** <*starting-time*>

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **end** <*ending-time*>

The following example configures a time range, which ranges from 8:00 to 18:00 during weekly working hours.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
admin@Xorplus# commit
admin@Xorplus# run show timerange timerange1234
TimeRange: timerange1234
Periodic: 400
    Week: weekdays, start:08:00:00, end:18:00:00
```

NOTEs:

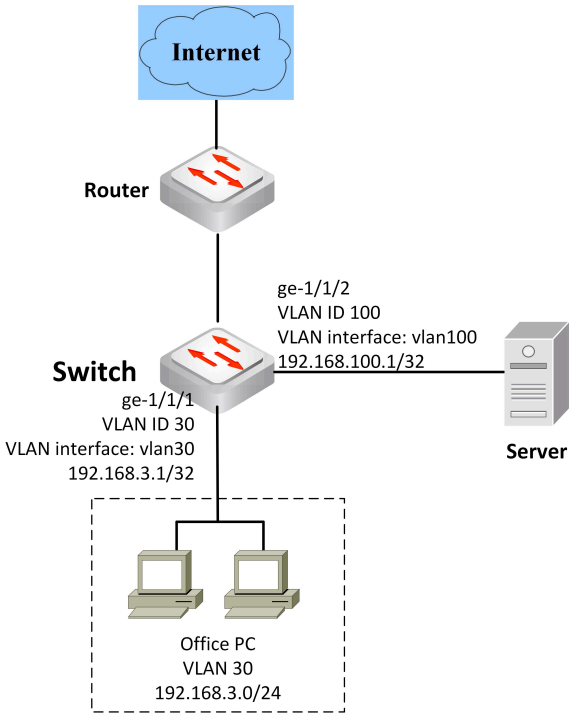
- A pair of start time and end time forms a time range.
- Currently only one **periodic** can be configured under a **time range**. However, multiple time periods can be configured under one **periodic**. All the time periods under the same time range take effect.
- In the same **periodic**, you cannot configure **daily**, **weekdays**, **weekend** at the same time.

```
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays start 8:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays end 18:00:00
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily start 1:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily end 3:00:00
admin@Xorplus# commit
Commit OK.
```

Example for Configuring ACL Rule of Time Range

Networking Requirements

Figure 1. Example for Configuring ACL Rule of Time Range



As shown in **Figure 1**, Office PCs access the Internet and the company Server through Switch. To restrict Office PCs to access the company Server only during business hours (08:00-18:00) on weekdays, configure filtering conditions of time range, source address and destination address of a ACL rule to achieve this requirement.

Procedure

The following are the configuration steps on the device Switch.

Step 1 Configure VLANs and VLAN interfaces.

```
admin@Switch# set vlans vlan-id 30
admin@Switch# set vlans vlan-id 100
admin@Switch# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 30
admin@Switch# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 100
admin@Switch# set vlans vlan-id 30 l3-interface vlan30
admin@Switch# set vlans vlan-id 100 l3-interface vlan100
admin@Switch# set l3-interface vlan-interface vlan30 address 192.168.3.1 prefix-length 32
admin@Switch# set l3-interface vlan-interface vlan100 address 192.168.100.1 prefix-length 32
```

Step 2 Configure time range.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
```

Step 3 Configure ACL rule.

```
admin@Switch# set firewall filter f1 sequence 1 from destination-address-ipv4 192.168.100.1/32
admin@Switch# set firewall filter f1 sequence 1 from source-address-ipv4 192.168.3.0/24
admin@Switch# set firewall filter f1 sequence 1 from time-range timerange1234
admin@Switch# set firewall filter f1 sequence 1 then action forward
```

Step 4 Apply the ACL filter rules to the access port.

```
admin@Switch# set firewall filter f1 input interface ge-1/1/1
```

Step 5 Commit the configurations.

```
admin@Switch# commit
```

Verify Configuration

- On Switch, run command **run show timerange** to view the configuration information about time range.

```
admin@Switch# run show timerange timerange1234
TimeRange: timerange1234
Periodic: 400
    Week: weekdays, start:08:00:00, end:18:00:00
```

- On Switch, run command **run show filter** to view the information about the ACL filter rule.

```
admin@Switch# run show filter f1
Filter: f1
    Description:
    Sequence: 1
        Description:
        match counter:  0 packets
        match-condition:
            destination-address-ipv4: 192.168.100.1/32
            source-address-ipv4:    192.168.3.0/24
            time-range:            timerange1234
        action: forward
        forwarding_class:
    Input interface: ge-1/1/1
```

QoS Configuration

This chapter describes Layer2 and Layer3 QoS configurations.

- Weighted Random Early Detection
  - WRED Overview
  - WRED Configuration Tasks
  - WRED Configuration Example
- QoS Principle
- SP Configuration Example
- QoS Configuration Example
  - Configuring Classifier-based QoS
  - Configuring ACL-based QoS
- PFC Configuration Example
- ACL-based Traffic Policer
- CoPP Configuration Guide
  - Principle
  - Default Settings for CoPP (N2224PX-ON/N2248X-ON/N3208PX-ON)
  - CoPP Configuration
    - Configuration Notes
    - Configuring CoPP
    - Configuration Example
  - Default Settings for CoPP
- Queue-based Rate Limiting
- Interface-based Rate Limiting
  - Configuring Ingress Interface-based Rate Limiting
  - Configuring Egress Interface-based Rate Limiting
- WRR Configuration Example
- Buffer Management
- WFQ Configuration Example

Weighted Random Early Detection

WRED (Weighted Random Early Detection) is a congestion avoidance mechanism that makes use of the congestion control mechanism of TCP (Transmission Control Protocol). By selectively dropping packets before periods of congestion, WRED tells TCP senders to reduce their transmission rates.

This chapter provides an overview of WRED, describes WRED configuration tasks, and presents a configuration example.

- WRED Overview
- WRED Configuration Tasks
- WRED Configuration Example

WRED Overview

You can monitor the network traffic load on an interface to anticipate congestion. Congestion can be avoided by dropping packets when needed. Tail drop is the most basic mechanism for avoiding congestion. Interface output queues fill during periods of congestion. When an output queue is full, the tail drop mechanism kicks in, and packets are dropped from the tail of the queue until congestion is reduced and the queue is no longer full. Tail drop does not differentiate between classes of traffic and drops packets at the tail of an output queue indiscriminately.

Global synchronization is a problem that occurs when tail drop is used as the congestion avoidance mechanism. Tail drop results in a large number of packets getting dropped at once. In response to packet drops, multiple senders of TCP (Transmission Control Protocol) traffic reduce their transmission rates at around the same time. The same TCP senders then increase their transmission rates around the same time when congestion is reduced. It results in periods of high link utilization followed by periods of low utilization.

WRED (Weighted Random Early Detection) is a congestion avoidance mechanism that prevents the problem of global synchronization associated with tail drop. When an output queue begins to experience congestion, WRED starts dropping packets *selectively*. A TCP sender experiencing packet drops reduces its transmission rate. By dropping some packets earlier than the point when the queue is full, WRED prevents the situation where a large number of packets get dropped at once. WRED not only reduces the chances of global synchronization, it also increases the utilization of transmission bandwidth.

WRED should be configured on egress ports.

WRED Configuration Tasks

When a packet arrives at a WRED-enabled output interface, the following chain of events takes place:

1. The length of the queue is calculated.
2. If the queue length is less than the minimum threshold, the packet is placed in the queue.
3. If the queue length is more than the maximum threshold, the packet is dropped.
4. If the queue length is more than the minimum threshold but less than the maximum threshold, the packet is either dropped or queued, based on the packet drop probability.

The following command can be used to enable or disable WRED:

set interface gigabit-ethernet <*port*> **wred queue** <*value*> **enable** <*bool*>

The following example demonstrates how to enable WRED on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 enable true
admin@XorPlus# commit
Commit OK.
Save done.
```

The following example demonstrates how to disable WRED on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 enable false
admin@XorPlus# commit
Commit OK.
Save done.
```

The following command can be used to set the maximum threshold:

set interface gigabit-ethernet <*port*> **wred queue** <*value*> **max_thresh** <*int*>

The following example demonstrates how to set the maximum threshold to 400 on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 max_thresh 400
admin@XorPlus# commit
Commit OK.
Save done.
```

The following command can be used to set the minimum threshold:

set interface gigabit-ethernet <*port*> **wred queue** <*value*> **min_thresh** <*int*>

The following example demonstrates how to set the minimum threshold to 200 on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 min_thresh 200
admin@XorPlus# commit
Commit OK.
Save done.
```

The following command can be used to to configure drop probability:

set interface gigabit-ethernet <*port*> **wred queue** <*value*> **drop_probability** <*int*>

The following example demonstrates how to set the drop probability to 50% on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 drop_probability 50
admin@XorPlus# commit
Commit OK.
Save done.
```

When congestion occurs, WRED drops packets based on the queue length exceeding certain threshold value. ECN (Explicit Congestion Notification) can enhance basic WRED operation by marking packets instead of dropping them when the queue length exceeds certain threshold value. Downstream routers and hosts would see this marking as an indication of network congestion and slow down their packet transmission rates.

ECN is a value in the DS (Differentiated Services) field of the IPv4 protocol header. ECN uses the two least significant (right-most) bits of the 8-bit DF field to encode four different codepoints:

1. 00 - Not ECN-Capable Transport
2. 01 - ECN-Capable Transport(1)
3. 10 - ECN-Capable Transport(0)
4. 11 - Congestion Experienced

When both end hosts support ECN, they mark their packets with either 10 or 01. When ECN is enabled, PicOS changes the ECN field of all such packets to 11. When ECN is not enabled, the ECN bits are not changed.

The following command can be used to enable or disable ECN:

set interface gigabit-ethernet <*port*> **wred queue** <*value*> **ecn_thresh** <*int*>

The following example demonstrates how to enable ECN on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 ecn_thresh 1
admin@XorPlus# commit
Commit OK.
Save done.
```

The following example demonstrates how to disable ECN on queue 0 of interface ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 wred queue 0 ecn_thresh 0
admin@XorPlus# commit
Commit OK.
Save done.
```

WRED Configuration Example

As shown in Fig 1, interfaces ge-1/1/1, ge-1/1/2, and ge-1/1/3 are connected to end hosts PC1, PC2, and PC3, respectively. Ports ge-1/1/1 and ge-1/1/12 are ingress ports, while ge-1/1/3 is an egress port. In this example, WRED is configured on ge-1/1/3.

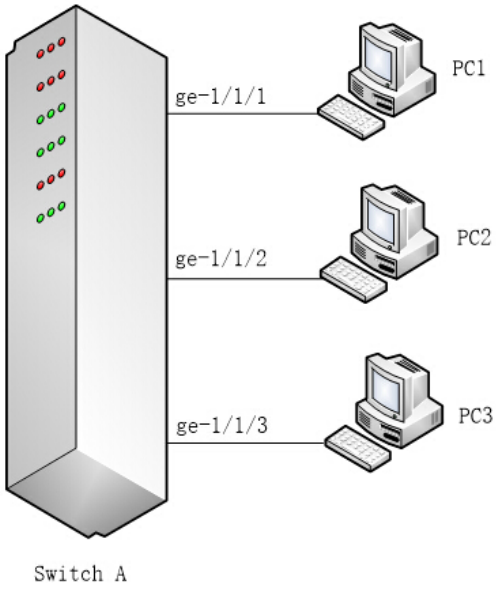


Fig 1. Configure WRED

Enable WRED

Enable WRED on queue 0 of interface ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 0 enable true
admin@XorPlus# commit
Commit OK.
Save done.
```

Set Maximum and Minimum Thresholds

Set the maximum threshold to 400 and the minimum threshold to 200 on queue 0 of interface ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 0 max_thresh 400
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 0 min_thresh 200
admin@XorPlus# commit
Commit OK.
Save done.
```

Set Drop Probability

Set the drop probability to 50% on queue 0 of interface ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 0 drop_probability 50
admin@XorPlus# commit
Commit OK.
Save done.
```

Enable ECN

Enable ECN (Explicit Congestion Notification) on queue 0 of interface ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 0 ecn_thresh 1
```

```
admin@XorPlus# commit
Commit OK.
Save done.
```

QoS Principle

SP Queue Principle

When the scheduler mode is SP, the egress port has eight queues: 7, 6, 5, 4, 3, 2, 1, and 0, queue 7 being the highest priority and queue 0 being the lowest priority. The advantage is that it can give priority to the transmissions of a key business group. This scheduler mode also has disadvantages. During times of congested conditions, if higher the priority queue has groups for a long time, the low priority queues will not get service all the time.

WRR Principle

The full name of WRR is Weighted Round Robin. In order to ensure that every queue has certain servicing time, WRR uses a round robin scheduling algorithm between the queues. When the scheduler mode is WRR, every queue can have a weighted value, which is also known as scheduling weight. Scheduling weight means that when the egress port schedules, the queue messages the proportion of scheduling resources to be used. Scheduling unit is Kbps.The example of a WRR scheduling algorithm is as follows:

On the 1000 Mbps egress port, the scheduling weights of eight queues are 5, 4, 3, 3, 2, 1, 1, 1; this ensures that even the lowest priority queue gets bandwidth.

The calculation method is as follows:

1/(5+4+3+3+2+1+1+1)*1000 Mbps=50 Mbps.

This can avoid the problem of the packets in the lower priority queues not getting service for a long time. The advantage is that although the queue scheduling uses round robin scheduling, every queue does not distribute at a fixed service time—if a queue is empty, the next queue should be scheduled immediately. In this way, it makes full use of bandwidth resources. When using WRR scheduling mode, user can define the weighted value for each queue.

WFQ Principle

The full name of WFQ is Weighted Fair Queuing. It is similar to WRR. The only difference between WFQ and WRR is that the scheduling mode in WFQ supports a minimum bandwidth guarantee, making this scheduling scheme more flexible. Configuring a minimum guaranteed bandwidth assures that every queue working in WFQ mode has a minimum bandwidth guarantee. In addition, the bandwidth available for distribution allocates according to the weighted proportion in the corresponding queue.

The distributable bandwidth calculation method is as follows:

distributable bandwidth = total bandwidth - minimum bandwidth

The example of the WFQ scheduling algorithm as follows:

Assuming that the total bandwidth of the egress port is 100M, there are 3 flows in the queue of this port.

Their scheduling weighted values are 1,2,4; the minimum bandwidth guarantees of these 3 flows are 10000Kbps,10000Kbps, and 20000Kbps.

Proportions of each flow are 10%,10%, 20%.

Distributable bandwidth = 100M-(10M+10M+20M)=60M.

Proportion of distributable bandwidth is 60%

Total distributable bandwidth = the sum of each flow weighted value.

In this example, the total distributable bandwidth is 7(that is 1+2+4).

Formula to calculate the proportion of distributable bandwidth which is occupied by each flow is as follows:

Proportion of distributable bandwidth = (the own weight of flow)/(distributable bandwidth).

Proportions of the distributable bandwidth for each flow are 1/7, 2/7, 4/7.

Bandwidth ratio of the flows is (10%+60%*(1/7)) : (10%+60%*(2/7)) : (20%+60%*(4/7)),that is 13:19:38.

SP Configuration Example

As shown in Fig 1, ge-1/1/1 and ge-1/1/2 are ingress ports, and ge-1/1/3 is an egress port. Use default scheduling model: priority trust model is IEEE 802.1.

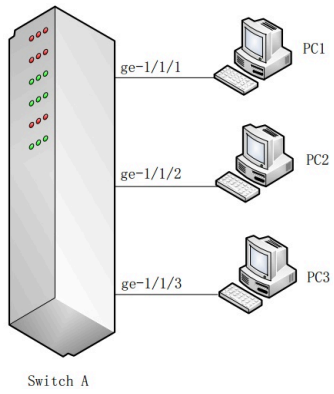


Fig 1. Configure SP

Configure two forwarding-classes

Configure forwarding-class f1 and f2 and their local-priorities.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 3
admin@XorPlus# set class-of-service forwarding-class f2 local-priority 6
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring classifier

Configure classifier c1, c2, and trust mode. Also configure classifier relevant to forwarding class and code point.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 5
admin@XorPlus# set class-of-service classifier c2 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c2 forwarding-class f2 code-point 7
admin@XorPlus# commit
Commit OK.
Save done.
```

Apply classifiers to two ingress ports

Configure classifier c1 and apply it to port ge-1/1/1. Configure classifier c2 and apply it to port ge-1/1/2.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# set class-of-service interface ge-1/1/2 classifier c2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
802.1P       Priority Flow Control  RxPFC          TxPFC
-----------  --------------------  -------------- ---------------
0            false                 0              0
1            false                 0              0
2            false                 0              0
3            false                 0              0
```

```
4            false                0              0
5            false                0              0
6            false                0              0
7            false                0              0

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                    0
1                SP,0kbps                    1
2                SP,0kbps                    2
3                SP,0kbps                    3,5
4                SP,0kbps                    4
5                SP,0kbps
6                SP,0kbps                    6
7                SP,0kbps                    7

admin@XorPlus# run show class-of-service interface ge-1/1/2
Interface : ge-1/1/2
802.1P       Priority Flow Control RxPFC           TxPFC
------------ -------------------- -------------- ---------------
0            false                0              0
1            false                0              0
2            false                0              0
3            false                0              0
4            false                0              0
5            false                0              0
6            false                0              0
7            false                0              0

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                    0
1                SP,0kbps                    1
2                SP,0kbps                    2
3                SP,0kbps                    3
4                SP,0kbps                    4
5                SP,0kbps                    5
6                SP,0kbps                    6,7
7                SP,0kbps
```

Generate Traffic

PC1 and PC2 generates traffic, which is matched with the corresponding classifier. Port PC1 and PC2 send 100% traffic to PC3 at the same time.

The expected result is that PC3 only can receive packets from PC2.

QoS Configuration Example

- Configuring Classifier-based QoS
- Configuring ACL-based QoS

Configuring Classifier-based QoS

> **NOTE:**
> On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.

Configure a Scheduler

A scheduler, which determines the QoS working mode and weight, should be configured first when you configure QoS. The working mode can be SP, WRR, or WFQ, and the weight is 1 to 15.

SP is strictly a priority queue. When two PCs send 100% traffic to a same PC, all packets from the lower priority PC will be discarded. The default working mode is SP.

WRR is a weighted round robin queue, and under this mode, user can configure weight. If PCA and PCB sends 100% traffic to the same PCC, the PCC will receive packets from PCA and PCB according to the weight proportion in the corresponding queue.

WFQ is weighted fair queuing. Under this mode, user can configure guaranteed-rate and weight, and the guarantee is only available in WFQ mode. If PCA and PCB send 100% traffic to the same PCC, the PCC will receive packets from PCA and PCB according to the weight proportion and the guaranteed-rate in the corresponding queue.

```
admin@XorPlus# set class-of-service scheduler s1 mode WRR
admin@XorPlus# set class-of-service scheduler s1 weight 3
admin@XorPlus# commit
Commit OK.
Save done.
```

```
admin@XorPlus# set class-of-service scheduler s1 mode WFQ
admin@XorPlus# set class-of-service scheduler s1 weight 4
admin@XorPlus# set class-of-service scheduler s1 guaranteed-rate 8
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure a Forwarding Class

A forwarding class, which determines the queue number of the specified traffic type, should be configured after the scheduler when configuring QoS. The effective local-priority is 0 to 7.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 3
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Scheduler Profile

Scheduler profile, which defines a queue used as a kind of scheduler on egress port, is the map of a forwarding class and a scheduler.

```
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f1 scheduler s1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Scheduler Profile to Specified Port

Scheduler profile should be configured to egress port. It only applies to egress packet. Ingress packet is invalid.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 scheduler-profile p1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure a Classifier with IEEE 802.1/DSCP/ToS

A classifier should be configured first, which is used to specify the associated forwarding class. User can select a classifier trust mode, such as IEEE 802.1, DSCP, or ToS, according to need. It decides the priority trust model. Configure trust mode IEEE 802.1 as follows:

```
admin@XorPlus# set class-of-service classifier c1 trust-mode ieee-802.1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Classifier Relevant to Forwarding Class

After configuring a classifier trust mode, user can configure the classifier relevant to the specified forwarding class. Code point and scheduler should be configured at the same time. The code-point is matched with the forwarding class local-priority, meaning that when the flow matches the specified code point, the flow will enter the specified queue. When the classifier trust mode is IEEE 802.1 or ToS, the code point is 0 to 7. When the classifier trust mode is dscp, the code point is 0 to 63.

```
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 5
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Classifier to Specified Port

After configuring as above, the classifier should be applied to specified ports. It determines the port priority trust model, data stream and queue matching rules, scheduling model, weight, and guaranteed-rate. When the classifier configures the scheduler, the classifier should be used in the egress port. When the classifier configures code point, the classifier should be used in ingress port.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring ACL-based QoS

NOTE:

On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.

Procedure

Step1 Configure firewall filter rule for traffic classification.

set firewall filter <*filter-name*> **sequence** <*number*> **from destination-mac-address** <*mac-address*>

NOTE:

- The matching fields of firewall filter rule could be **destination-mac-address**, **source-mac-address**, **destination-address-ipv4** (for IPv4 matching rule), **destination-address-ipv6** (for IPv6 matching rule), **source-address-ipv4** (for IPv4 matching rule), **source-address-ipv6** (for IPv6 matching rule), **protocol**, **destination-port**, **source-port**, **ether-type**, **vlan**, **ip trust-mode**, **ip value**.
- **and** is the logical operator between the matching fields with the same sequence number, that is, packets must match all of the matching fields with the same sequence number to be included in one class.

Step2 Configure queue mapping between firewall filter and forwarding class.

set firewall filter <*filter-name*> **sequence** <*number*> **then forwarding-class** <*forwarding-class-name*>

Step3 Configure DSCP remark.

set firewall filter <*filter-name*> **sequence** <*number*> **then dscp** <*dscp-value*>

Step4 Apply firewall filter to a switch physical interface.

set firewall filter <*filter-name*> **input interface** <*interface-name*>

Step5 Configure mapping between forwarding class and local priority.

set class-of-service forwarding-class <*forwarding-class-name*> **local-priority <***int*>

Step6 Configure queue scheduler weight.

set class-of-service scheduler <*scheduler-name*> **weight** <*int*>

Step7 Configure WRR scheduling algorithm for queue scheduling.

set class-of-service scheduler <*scheduler-name*> **mode** <**SP | WFQ | WRR>**

Step8 Configure guaranteed-rate for queue.

set class-of-service scheduler <*scheduler-name*> **guaranteed-rate** <*value*>

Step9 Configure scheduler profile.

set class-of-service scheduler-profile <*scheduler-profile-name***> forwarding-class** <*forwarding-class-name*> **scheduler <***scheduler-name*>

Step10 Apply scheduler profile to a switch physical interface.

set class-of–service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>

Step11 Commit the configuration.

commit

Configuration Example

The following example configures ACL-based QoS policy for NTP protocol, and applies it to the interface ge-1/1/1.

Procedure

Step1 Configure destination-port, protocol and ether-type to classify NTP (Network Time Protocol) flow, and mapping to forwarding class class1.

```
admin@Xorplus# set firewall filter f1 sequence 91 from destination-port 123
admin@Xorplus# set firewall filter f1 sequence 91 from protocol udp
admin@Xorplus# set firewall filter f1 sequence 91 then forwarding-class class1

admin@Xorplus# set firewall filter f1 sequence 92 from destination-port 123
admin@Xorplus# set firewall filter f1 sequence 92 from ether-type 34525
admin@Xorplus# set firewall filter f1 sequence 92 from protocol udp
admin@Xorplus# set firewall filter f1 sequence 92 then forwarding-class class1
```

Step2 Configure CoPP queue mapping, scheduling weight, scheduling algorithm and queue guaranteed-rate.

```
admin@Xorplus# set class-of-service scheduler scheduler180 mode WFQ
admin@Xorplus# set class-of-service scheduler scheduler180 guaranteed-rate 10000
admin@Xorplus# set class-of-service scheduler scheduler180 weight 5
admin@Xorplus# set class-of-service scheduler-profile s1 forwarding-class class1 scheduler scheduler180

##Configure mapping between forwarding class and local priority.
admin@Xorplus# set class-of-service forwarding-class class1 local-priority 1
```

Step3 Apply firewall filter to a switch physical interface.

```
  admin@XorPlus# set firewall filter f1 input interface ge-1/1/1
```

Step4 Apply scheduler profile to a switch physical interface.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 scheduler-profile s1
```

Step5 Commit the configuration.

```
admin@XorPlus# commit
```

Verify the Configuration

- You can use the **run show filter** command to view the configuration information of all firewall filter rules.

```
admin@XorPlus# run show filter
```

```
Filter: f1
    Description:
    Sequence: 91
        Description:
        match counter:  0 packets
        match-condition:
            destination-port:         123..123
            protocol:                 udp
        action: forward
        forwarding_class: classs1
    Sequence: 92
        Description:
        match counter:  0 packets
        match-condition:
            destination-port:         123..123
            ether-type:               0x86dd
            protocol:                 udp
        action: forward
        forwarding_class: classs1
    Input interface: ge-1/1/1
```

- You can use the **run show class-of-service** command to view the information of ACL-based QoS configuration information.

```
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule         Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps
1                WFQ,5,10000kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

PFC Configuration Example

Priority Flow Control or PFC is a kind of flow control mechanism. The advantage of PFC over traditional Flow Control mechanisms is that PFC provides flow control based on per code point (priority). In other words, PFC provides a more granular form of flow control. This means that if traffic from one particular priority suffers from congestion, only that traffic is paused until congestion clears away, whereas traffic for other priorities continues unhindered. On each physical port, there are 8 (0 to 7) Class of Service (CoS) queues, if congestion is detected on the egress physical port, the ingress port will send a PAUSE frame to the transmitting node to pause transmission until the receiving node is ready to accept packets again. PFC applies only to packets entering a port.

PFC has a higher priority than flow control. So, for example, if both flow control and PFC are configured on the same port, PFC will have precedence over traditional flow control.

PFC uses the IEEE 802.1p CoS values in the IEEE 802.1Q VLAN tag to generate the flow control frame with corresponding priority on ingress physical port when egress physical port suffers congestion. It indicates the ingress port needs COS classifier configuration.

PFC configuration is applied using PFC profiles. The following is an example of PFC configuration.

Configure PFC Profile

PFC is disabled when drop value is set to true and enabled when drop value is set to false. The default value of drop is false.

For example as below, PFC is enabled on 0，1，3，5，6，7 code-point by default, PFC is disabled on 2，4 code-point.

```
admin@XorPlus# set class-of-service pfc-profile pfc1 code-point 2 drop true
admin@XorPlus# set class-of-service pfc-profile pfc1 code-point 4 drop true
admin@XorPlus# commit
Commit OK.
Save done.
```

Apply PFC Profile to Port

```
admin@XorPlus# set class-of-service interface ge-1/1/1 pfc-profile pfc1
admin@XorPlus# commit
Commit OK.
Save done.
```

Show PFC Frame Statistics on Port

The class 0~7 in PFC frame corresponds to the following "802.1P" item. The value of "RxPFC“ item will be incremented by 1 if ge-1/1/1 receives a PFC frame. The value of "TxPFC“ item will be incremented by 1 if ge-1/1/1 sends out a PFC frame.

```
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
802.1P         Priority Flow Control    RxPFC              TxPFC
-----------    ---------------------    ---------------    ---------------
0              true                     0                  0
1              true                     0                  0
2              false                    0                  0
3              true                     0                  0
4              false                    0                  0
5              true                     0                  0
6              true                     0                  0
7              true                     0                  0
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule               Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

Apply classifier based on IEEE 802.1P to ingress port

```
admin@XorPlus# set class-of-service classifier c1
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
802.1P         Priority Flow Control    RxPFC              TxPFC
-----------    ---------------------    ---------------    ---------------
0              true                     0                  0
1              true                     0                  0
2              false                    0                  0
3              true                     0                  0
4              false                    0                  0
5              true                     0                  0
6              true                     0                  0
7              true                     0                  0
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule               Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps                           0
1                SP,0kbps                           1
2                SP,0kbps                           2
3                SP,0kbps                           3
4                SP,0kbps                           4
5                SP,0kbps                           5
6                SP,0kbps                           6
7                SP,0kbps                          7
```

ACL-based Traffic Policer

- ACL-based Traffic Policer Implementation
- Rate-limit and Burst Applied in ACL-based Traffic Policer Function
- Interoperability with CoPP Policy
- Configuring ACL-based Traffic Policer
- Configuration Example

ACL-based traffic policer provides the ability to monitor the data rates for a particular class of traffic, and drops the traffic that exceed the user-configured rate-limit and burst limit values.

ACL-based traffic policer defines a rate limiting policy including traffic classification using ACL rules and policer (rate limit, burst limit and action) which can be applied to the management interface(eth0 / eth1) or an Ethernet interface to control the packet bandwidth in or out of the interface.

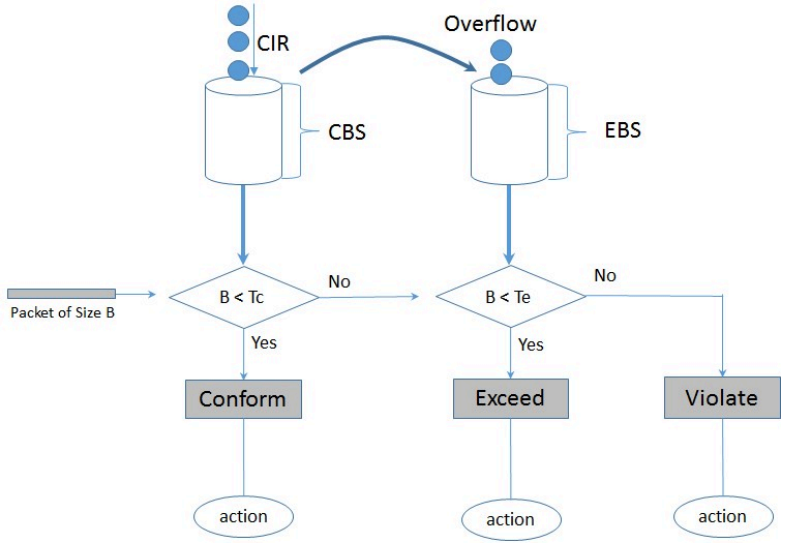
ACL-based Traffic Policer Implementation

When configured the ACL-based traffic policer on PICA8 switch, the sequence of packets processing is as follows:

1. A packet enters the switch configured with ACL-based traffic policer on the ingress port.
2. PICOS performs any applicable firewall filter services on the ingress port.
3. Packets are processed by ACL-based traffic policer module and are dropped or forwarded according to each firewall filter policy.
4. The forwarded packet is sent to the switch CPU if it is destined for the switch CPU.
5. The switch CPU makes a routing or switching decision, determining whether the packet is should be dropped or forwarded.
6. Packets that have destinations other than CPU are forwarded normally.

Rate-limit and Burst Applied in ACL-based Traffic Policer Function

Figure 1. RFC2697 Single-Rate Three-Color Policer Logic



The single-rate three-color policer/marker algorithm with dual buckets is used to implement ACL- based traffic policer rate-limit and burst-limit. Unlike the standard algorithm, the yellow traffic will be discarded as well as red traffic in order to make the implementation simple enough.

Additionally, the action to be applied to a packet, forward or discard, totally depends on the Tc, the token counter of CBS, the instantaneous number of tokens left in the CBS bucket because both yellow and red traffic will be discarded for PICA8 switch, which means the second bucket - EBS bucket - is not used to police the traffic at all.

For example:

set firewall policer 10pps if-exceeding count-mode packet

set firewall policer 10pps if-exceeding rate-limit 10

set firewall policer 10pps if-exceeding burst-limit 5

The above configuration is equal to below :

CIR (Committed Information Rate): 10 pps

CBS (Committed Burst Size): 5 packet

EBS (Excess Burst Size): 5 packet

10 pps is rate-limit value, 5 packet is burst value, the size of the bucket.

Interoperability with CoPP Policy

ACL-based traffic policer can take effect on packets that are both directed and non-directed to the CPU. The CoPP policy takes effect only on the packets directed to the CPU. These are independent functions. You can configure only one of them, or both of them.

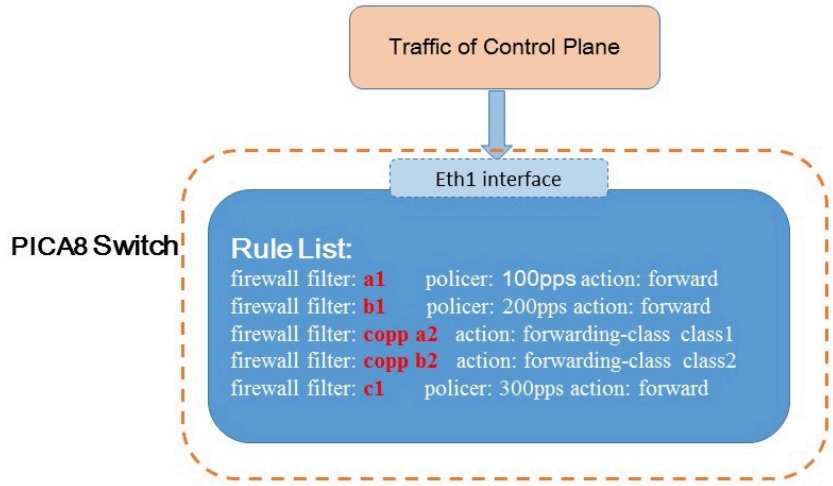
If both ACL-based traffic policer and the COPP policy are configured, for the packets directed to the CPU, the system processing is different in the following two cases: both the policies are applied to the same management interface or both the policies are applied to the same Ethernet interface.

1. When both ACL-based traffic policer and COPP policy are applied to the same management interface.

   In this case, the ACL-based traffic policer and the CoPP policy are in the same rule list in which the rules are ordered by the firewall filter name (for example, firewall filter with name "**a_filter**" is in front of "**b_filter**". Firewall filter name of CoPP policy is fixed to "copp"). The packets are matched against the rules in the ascending order.

   When the configured ACL-based traffic policer conflicts with the CoPP policy, first matched policy takes effect and the other policy will not take effect. Therefore, it is recommended not to configure conflicted ACL-based traffic policer with the CoPP policy.

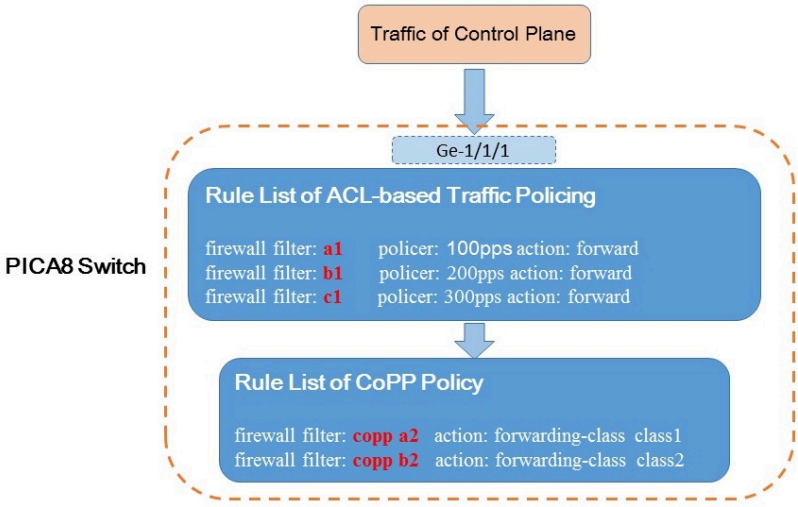
Figure 2. ACL-based traffic policer rules and CoPP policy rules are put in the same rule list



2. When both ACL-based traffic policer and COPP policy are applied to the same Ethernet interface.

   For the packets directed to the CPU, the packet is processed by the ACL-based traffic policer module first, and then is processed by the COPP policy module.

Figure 3. ACL-based traffic policer and CoPP policy are performed one by one



Configuring ACL-based Traffic Policer

NOTE:

- The filter can be configured on one or several interfaces in the inbound and outbound directions. However, a single filter can be configured either in the inbound direction or outbound direction at any given time.
- One policer can be applied to one filter. We can configure one policer on one or several sequences of a filter.
- Multiple sequences of the same filter share the rate limit and burst-limit of the policer. That is, when you configure the same policer to multiple sequences of the same filter, the packets matching the sequence condition of the filter can share the bandwidth rate limit and burst-limit of the policer, following the order in which the traffic arrives.

Step1 Configure ACL-based traffic policer rate-limit and burst-limit.

set firewall policer *<policer-name>* **if-exceeding count-mode** *<count-mode>*

set firewall policer <*policer-name*> **if-exceeding rate-limit** <*value*>

set firewall policer <*policer-name*> **if-exceeding burst-limit** <*value*>

Step2 Configure ACL-based traffic policer action as **discard**. The default action is **discard** if not configured.

set firewall policer <*policer-name*> **then action discard**

Step3 Configure firewall filter match condition and the policer for packets matching a filter sequence.

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **from** <*match-conditions*>

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **then policer** <*policer-name*>
set firewall filter <*filter-name*> **sequence** <*sequence-number*> **then action** {**discard** | **forward**}

Step4 Configure firewall filter applied to an Ethernet interface or a Layer 3 VLAN interface in the inbound or outbound direction.

set firewall filter <*filer-name*> **input interface** <*interface-name*>

set firewall filter <*filter-name*> **output interface** <*interface-name*>

set firewall filter <*filter-name*> **input vlan-interface** <*vlan-interface-name*>

set firewall filter <*filter-name*> **output vlan-interface** <*vlan-interface-name*>

Configuration Example

The following example configures ACL-based traffic policer for ICMP protocol packets and applies to the management port Eth1.

Step1 Configure ACL-based traffic policer rate-limit and burst-limit.

```
admin@Switch# set firewall policer 100pps if-exceeding count-mode packet
admin@Switch# set firewall policer 100pps if-exceeding rate-limit 100
admin@Switch# set firewall policer 100pps if-exceeding burst-limit 5
admin@Switch# set firewall policer 100pps then action discard
```

Step2 Configure firewall filter match and applied policer to firewall filter action.

```
admin@Switch# set firewall filter f1 sequence 1 from protocol icmp
admin@Switch# set firewall filter f1 sequence 1 then policer 100pps
admin@Switch# set firewall filter f1 sequence 1 then action forward
```

Step3 Configure firewall filter applied to the management interface eth1.

```
admin@Switch# set firewall filter f1 input interface eth1
```

Step4 Commit the configuration.

```
admin@Switch# commit
```

Step5 Run **run show policer** command to check the configuration.

```
admin@Switch# run show policer
policer     rate limit   burst limit   count mode   action
------------   ----------    ----------     ----------    ----------
100pps         100          5             packet         discard
```

CoPP Configuration Guide

- Principle
- Default Settings for CoPP (N2224PX-ON/N2248X-ON/N3208PX-ON)
- CoPP Configuration
  - Configuration Notes
  - Configuring CoPP
  - Configuration Example
- Default Settings for CoPP

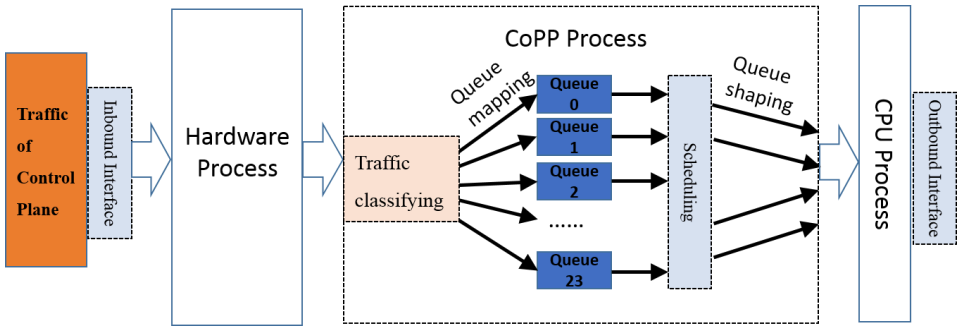
Principle

- Definition
- CoPP Traffic Classification
- Queue Mapping and Scheduling
  - Queue Mapping
  - Scheduling
- Queue Shaping

Definition

Control Plane Policing (CoPP) defines the traffic classification, queue mapping, and queue shaping for control plane packets directed to switch CPU, achieving to protect switch from being overwhelmed by malicious attacks and overload, maintaining data forwarding and network topology stability. CoPP uses a dedicated control plane configuration through the QoS module of CoS (Class of Service) and Firewall Filter Rule. **Figure 1** shows the CoPP process.

Figure 1 CoPP Process



CoPP process follows four steps:

Classifying: CoPP identifies and classifies the flow of traffic handled by the switch CPU according to packet information of layer 2, layer 3 and layer4 based on firewall filter rules.

Queue mapping: This action is responsible for sending different types of packets to the specified CPU queue. The packets in different queues have different scheduling priorities according to scheduling weight.

Scheduling: When a network is congested intermittently and delay-sensitive services require higher bandwidth than other services, or when there are packets in multiple queues to be transmitted, scheduling is responsible for selecting a queue with a scheduling algorithm and processing the packets from the queue. CoPP uses the Weighted Round Robin (WRR) scheduling algorithm; please refer to 1.1.3 Queue Mapping and Scheduling for details about WRR.

Queue shaping: Set a minimum and maximum bandwidth for each CPU queue in packets per second (PPS) for queue shaping, this queue bandwidth limit ensures that the CPU will not face excessively loaded conditions in any case.

CoPP Traffic Classification

Based on the firewall filter rules, control plane packets directed to switch CPU are checked to see whether they hit a matching field specified in the firewall filter rules. If the packet matches a specified matching field, it is considered a member of a class and maps to a specified CPU queue according to the queue mapping policy.

and is the logical operator between the matching fields with the same sequence number, that is, to be considered to match a firewall filter rule and included in a class, the packets must match all of the matching fields with the same sequence number.

CoPP supports both IPv4 and IPv6 firewall filters, the descriptions of the supported matching fields are as follows:

- **Destination-mac-address/source-mac-address**: Filter packets with a specific destination/source MAC address.
- **Destination-address-ipv4/source-address-ipv4**: Filter packets with a specific destination/source IPv4 address.
- **Destination-address-ipv6/source-address-ipv6**: Filter packets with a specific destination/source IPv6 address.
- **Protocol**: Protocol is the *Protocol* field of the IPv4 header and the *Next Header* field of the IPv6 header, it could be a protocol name or protocol number identifying the protocol type of packets. Assigned internet protocol numbers 8 for EGP, 9 for IGP, 47 for GRE, 88 for EIGRP, 103 for PIM, and 112 for VRRP are examples.
- **Destination-port/ Source-port**: Filter packets with a specific destination/source port.
- **Vlan**: A switch identifies packets from different VLANs by VLAN ID contained in VLAN tags in Ethernet frame. User can set VLAN ID in the firewall filter rule for traffic classification.
- **Ether-type**: Ether type is a two-octet field used for indicating which protocol is being transported in an Ethernet frame in the Ethernet networking standard. Table 1 shows the Ether type value of the common protocols.

Table 1 Ether Type value of the common protocols

Protocol Type	Ether Type(Hexadecimal)
Internet Protocol, Version 4 (IPv4)	0x0800
Address Resolution Protocol (ARP)	0x0806

Protocol Type	Ether Type(Hexadecimal)
Reverse Address Resolution Protocol (RARP)	0x8035
AppleTalk (Ethertalk)	0x809b
AppleTalk Address Resolution Protocol (AARP)	0x80f3
IEEE 802.1Q-tagged frame	0x8100
Novell IPX (alt)	0x8137
Novell	0x8138
Internet Protocol, Version 6 (IPv6)	0x86DD
Ethernet Slow Protocols	0x8809

Queue Mapping and Scheduling

Queue Mapping

With CoPP traffic classification, packets that match a firewall filter rule will be sent to a specified CPU queue according to the queue mapping policy.

If a packet matches no class for ACL action **discard** or **forward**, the match processing is as follows. Packet classification included within queue mapping policy is processed top-down. When a packet is found to match a class, no further match processing is performed. That is, a packet can only belong to a single class, and it is the first one to which a match occurs.

If a packet is found to match a class for ACL action **discard or forward**, the match processing is as follows:

- When a packet is found to match a class for action **discard**, then the switch will discard the packet and will not match the remaining ACLs.
- When a packet is found to match a class for action **forward**, then the switch will forward the packet according to the CoPP forward class firstly matched and will not match the remaining ACLs.

When a packet directed to switch CPU matches none of the defined firewall filter rule, it is automatically mapped to CPU queue 0.

The mapping relationships between the firewall filter rule and CPU queue are:

- One or more firewall filter rules can be mapped to one CPU queue (n to one mapping).
- Each firewall filter rules can be matched to at most one queue.

Scheduling

CoPP uses WRR (Weighted Round Robin) to schedule packets in queues.

In order to ensure every queue has certain servicing time, WRR uses a round robin scheduling algorithm between the queues. When the scheduler mode is WRR, every queue can have a weighted value, which is also known as scheduling weight. Scheduling weight implies that when the egress port schedules the queue messages a proportion of scheduling resources are to be used. Scheduling unit is Kbps. The example of a WRR scheduling algorithm is as follows:

On the 1000 Mbps egress port, the scheduling weights of eight queues are 5, 4, 3, 3, 2, 1, 1, 1; this ensures that even the lowest priority queue gets bandwidth.

The calculation method is as follows:

1/ (5+4+3+3+2+1+1+1)*1000 Mbps=50 Mbps.

This can help avoid the problem of packets in the lower priority queues not getting service for longer periods of time. The advantage is that although the queue scheduling uses round robin scheduling, every queue does not distribute at a fixed service time: if a queue is empty, the next queue should be scheduled immediately. In this way, it makes full use of bandwidth resources. When using WRR scheduling algorithm, user can define the weighted value for each queue.

Queue Shaping

Queue shaping adjusts the rate of traffic to switch CPU. It helps to reduce traffic bursts so that packets can be transmitted at a stable rate through to CPU. For queues of different priorities, the device can provide differentiated services using different queue shaping parameter settings of Max-bandwidth-pps and Min-bandwidth-pps.

- **Max-bandwidth-pps**: Max-bandwidth-pps is the maximum packet processing rate of a CPU queue in packets per second (PPS). If there is heavy traffic on the interface caused by malicious attacks or network exceptions, the CPU will be overloaded and services would be interrupted. In order to avoid this situation, user can set Maximum bandwidth to the CPU queue for queue shaping.
- **Min-bandwidth-pps**: Minimum bandwidth means a guaranteed bandwidth of CPU queue for packets in pps. The total value of min-bandwidth-pps of all activated queues should be less than CPU-affordable bandwidth, which should be the maximum bandwidth threshold to the CPU which is different depending on the platform.

Default Settings for CoPP (N2224PX-ON/N2248X-ON/N3208PX-ON)

Default Queue Mapping Policy
Default CLI Settings
Show Default Settings of CoPP

NOTE:

- Default settings for CoPP in this page is only applicable for N2224PX-ON/N2248X-ON/N3208PX-ON.
- CoPP configures control policy of the traffic from the ASIC to CPU. It is a very sensitive process of the whole switch OS. Any incorrect setting could impact the stability or could even paralyze the normal network operation. **It is therefore highly recommended to KEEP the default configurations of CoPP to ensure the system and network stability.**

Default Queue Mapping Policy

By default, CoPP provides 8 CPU queues for data forwarding that would have a default scheduling weight. The system pre-defines 15 types of control plane protocols mapping from queue 8 to 22. The default queue mapping policy is as follows.

Table 1. Default Queue Mapping Policy

Protocols	CPU Queue	Default Scheduling Weight
BPDU	7	32
LACP	6	32
LLDP	5	32
ARP/NDP	4	32
MLAG/MLAG-MAC-SYNC	3	16
SSH/TELNET/SNMP	2	32
DHCP/DHCPv6/IGMP/PIM	1	16
Default*	0	16

Default*: The flow of traffic directed to switch CPU will be sent to CPU queue 0 when the traffic matches no firewall filter rule.

But for the packet with an Inet Precedence or DSCP value, it will not always be sent to CPU queue 0 when the traffic matches no firewall filter rule. When you configure the classifier to classify services on different inbound interfaces by using **set class-of-service classifier trust-mode dscp** and **set class-of-service interface classifier** commands. The packets will be sent to the CPU queue according to the Inet Precedence or DSCP value. Mappings from Inet Precedence/DSCP value to CPU Queue are shown in the following tables.

Table 2. Mapping from Inet Precedence value to CPU Queue

Inet-precedence	CPU Queue
0	0

1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 3. Mapping from DSCP value to CPU Queue

DSCP	CPU Queue
0,1,2,3,4,5,6,7	0
8,9,10,11,12,13,14,15	1
16,17,18,19,20,21,22,23	2
24,25,26,27,28,29,30,31	3
32,33,34,35,36,37,38,39	4
40,41,42,43,44,45,46,47	5
48,49,50,51,52,53,54,55	6
56,57,58,59,60,61,62,63	7

Default CLI Settings

PicOS will startup with the following CLI commands by default. Users can change the pre-defined CoPP policies but are NOT allowed to delete them.

NOTE: The values of min-bandwidth-pps and max-bandwidth-pps are different on different platforms.

 # Default configurations of forwarding class for CoPP.

```
set class-of-service forwarding-class bpdu-class local-priority 7
set class-of-service forwarding-class lacp-class local-priority 6
set class-of-service forwarding-class lldp-class local-priority 5
set class-of-service forwarding-class arp-ndp-class local-priority 4
set class-of-service forwarding-class mlag-class local-priority 3
set class-of-service forwarding-class management-class local-priority 2
set class-of-service forwarding-class dhcp-igmp-pim-class local-priority 1
set class-of-service forwarding-class default-class local-priority 0
```

 # Default configurations of schedulers for CoPP.

```
set class-of-service scheduler arp-ndp-scheduler mode WRR
set class-of-service scheduler arp-ndp-scheduler weight 32
set class-of-service scheduler arp-ndp-scheduler max-bandwidth-pps 500
```

```
set class-of-service scheduler arp-ndp-scheduler min-bandwidth-pps 100


set class-of-service scheduler management-scheduler mode WRR
set class-of-service scheduler management-scheduler weight 32
set class-of-service scheduler management-scheduler max-bandwidth-pps 500
set class-of-service scheduler management-scheduler min-bandwidth-pps 100

set class-of-service scheduler dhcp-igmp-pim-scheduler mode WRR
set class-of-service scheduler dhcp-igmp-pim-scheduler weight 16
set class-of-service scheduler dhcp-igmp-pim-scheduler max-bandwidth-pps 500
set class-of-service scheduler dhcp-igmp-pim-scheduler min-bandwidth-pps 0

set class-of-service scheduler mlag-scheduler mode WRR
set class-of-service scheduler mlag-scheduler weight 16
set class-of-service scheduler mlag-scheduler max-bandwidth-pps 500
set class-of-service scheduler mlag-scheduler min-bandwidth-pps 0

set class-of-service scheduler bpdu-scheduler mode WRR
set class-of-service scheduler bpdu-scheduler weight 32
set class-of-service scheduler bpdu-scheduler max-bandwidth-pps 500
set class-of-service scheduler bpdu-scheduler min-bandwidth-pps 100

set class-of-service scheduler lacp-scheduler mode WRR
set class-of-service scheduler lacp-scheduler weight 32
set class-of-service scheduler lacp-scheduler max-bandwidth-pps 500
set class-of-service scheduler lacp-scheduler min-bandwidth-pps 100

set class-of-service scheduler lldp-scheduler mode WRR
set class-of-service scheduler lldp-scheduler weight 32
set class-of-service scheduler lldp-scheduler max-bandwidth-pps 500
set class-of-service scheduler lldp-scheduler min-bandwidth-pps 100

set class-of-service scheduler default-scheduler mode WRR
set class-of-service scheduler default-scheduler weight 16
set class-of-service scheduler default-scheduler max-bandwidth-pps 500
set class-of-service scheduler default-scheduler min-bandwidth-pps 0

set class-of-service scheduler-profile copp-profile forwarding-class bpdu-class
scheduler bpdu-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class lacp-class
scheduler lacp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class lldp-class
scheduler lldp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class dhcp-igmp-pim-
class scheduler dhcp-igmp-pim-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class mlag-class
scheduler mlag-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class management-
class scheduler management-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class arp-ndp-class
scheduler arp-ndp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class default-class
scheduler default-scheduler
```

 # Apply schedulers of CoPP to inbound interface.

```
set class-of-service interface inbound-control-plane scheduler-profile copp-profile
```

 # Default configurations of protocol sequences and forwarding class.

```
set firewall filter copp sequence 10 from protocol bpdu
set firewall filter copp sequence 10 then forwarding-class bpdu-class
set firewall filter copp sequence 20 from protocol lacp
set firewall filter copp sequence 20 then forwarding-class lacp-class
set firewall filter copp sequence 30 from protocol lldp
set firewall filter copp sequence 30 then forwarding-class lldp-class
set firewall filter copp sequence 40 from protocol arp
set firewall filter copp sequence 40 then forwarding-class arp-ndp-class
set firewall filter copp sequence 50 from protocol ndp
set firewall filter copp sequence 50 then forwarding-class arp-ndp-class
set firewall filter copp sequence 60 from protocol bfd
set firewall filter copp sequence 60 then forwarding-class default-class
set firewall filter copp sequence 70 from protocol mlag
set firewall filter copp sequence 70 then forwarding-class mlag-class
set firewall filter copp sequence 80 from protocol mlag-mac-sync
set firewall filter copp sequence 80 then forwarding-class mlag-class
set firewall filter copp sequence 90 from protocol bgp
set firewall filter copp sequence 90 then forwarding-class default-class
set firewall filter copp sequence 100 from protocol ospf
set firewall filter copp sequence 100 then forwarding-class default-class
set firewall filter copp sequence 110 from protocol rip
set firewall filter copp sequence 110 then forwarding-class default-class
set firewall filter copp sequence 120 from protocol dhcp
set firewall filter copp sequence 120 then forwarding-class dhcp-igmp-pim-class
set firewall filter copp sequence 130 from protocol vrrp
set firewall filter copp sequence 130 then forwarding-class default-class
set firewall filter copp sequence 140 from protocol igmp
set firewall filter copp sequence 140 then forwarding-class dhcp-igmp-pim-class
set firewall filter copp sequence 150 from protocol pim
set firewall filter copp sequence 150 then forwarding-class dhcp-igmp-pim-class
set firewall filter copp sequence 160 from protocol ssh
set firewall filter copp sequence 160 then forwarding-class management-class
set firewall filter copp sequence 170 from protocol telnet
set firewall filter copp sequence 170 then forwarding-class management-class
set firewall filter copp sequence 180 from protocol snmp
set firewall filter copp sequence 180 then forwarding-class management-class
```

#Apply firewall filter of CoPP to inbound interface.

```
set firewall filter copp input interface inbound-control-plane
```

Show Default Settings of CoPP

- You can use **run show copp bandwidth**, **run show class-of-service interface inbound-control-plane** and **run show filter copp** commands to view the default settings. (Besides default settings, the commands will also show the COPP configurations made by the user.)

```
admin@PICOS# run show copp bandwidth
Forwarding Class           Min-Bandwidth Max-Bandwidth Weight Local-Priority Schedule-Mode
```

```
default-class             0            500          16     0             WRR
dhcp-igmp-pim-class       0            500          16     1             WRR
management-class          100          500          12     2             WRR
mlag-class                0            500          16     3             WRR
arp-ndp-class             100          500          32     4             WRR
lldp-class                100          500          32     5             WRR
lacp-class                100          500          32     6             WRR
bpdu-class                100          500          32     7             WRR
```

```
admin@PICOS# run show filter copp
Filter: copp
    Description:
    Sequence: 10
        Description:
        match counter:  36415 packets
        match-condition:
            protocol:                bpdu
        action: forward
        forwarding_class: bpdu-class
    Sequence: 20
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                lacp
        action: forward
        forwarding_class: lacp-class
    Sequence: 30
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                lldp
        action: forward
        forwarding_class: lldp-class
    Sequence: 40
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                arp
        action: forward
        forwarding_class: arp-ndp-class
    Sequence: 50
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ndp
        action: forward
        forwarding_class: arp-ndp-class
    Sequence: 60
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                bfd
        action: forward
        forwarding_class: default-class
    Sequence: 70
        Description:
        match counter:  0 packets
        match-condition:
```

```
            protocol:                mlag
        action: forward
        forwarding_class: mlag-class
    Sequence: 80
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                mlag-mac-sync
        action: forward
        forwarding_class: mlag-class
    Sequence: 90
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                bgp
        action: forward
        forwarding_class: default-class
    Sequence: 100
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ospf
        action: forward
        forwarding_class: default-class
    Sequence: 110
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                rip
        action: forward
        forwarding_class: default-class
    Sequence: 120
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                dhcp
        action: forward
        forwarding_class: dhcp-igmp-pim-class
    Sequence: 130
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                vrrp
        action: forward
        forwarding_class: default-class
    Sequence: 140
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                igmp
        action: forward
        forwarding_class: dhcp-igmp-pim-class
    Sequence: 150
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                pim
        action: forward
```

```
        forwarding_class: dhcp-igmp-pim-class
    Sequence: 160
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ssh
        action: forward
        forwarding_class: management-class
    Sequence: 170
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                snmp
        action: forward
        forwarding_class: management-class
    Sequence: 180
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ntp
        action: forward
        forwarding_class: management-class
    Sequence: 190
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                tacacs
        action: forward
        forwarding_class: management-class
    Sequence: 200
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                radius
        action: forward
        forwarding_class: management-class
    Sequence: 210
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                mvrp
        action: forward
        forwarding_class: bpdu-class
    Sequence: 220
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                erps
        action: forward
        forwarding_class: bpdu-class
    Sequence: 230
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ripng
        action: forward
        forwarding_class: default-class
    Sequence: 240
```

```
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                loopback-detection
        action: forward
        forwarding_class: management-class
    Sequence: 260
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                isis
        action: forward
        forwarding_class: default-class
    Sequence: 270
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                dhcp6
        action: forward
        forwarding_class: dhcp-igmp-pim-class
    Input interface: inbound-control-plane

```

```
admin@PICOS# run show class-of-service interface inbound-control-plane
Interface : inbound-control-plane
Scheduler-profile : copp-profile
Forwarding-class     Local-priority   Scheduler               Min-Bandwidth   Max-Bandwidth   Weight   Schedule-Mode
------------------   --------------   ---------------------   -------------   -------------   ------   -------------
default-class        0                default-scheduler       0               500             16       WRR
dhcp-igmp-pim-class  1                dhcp-igmp-pim-scheduler 0               500             16       WRR
management-class     2                management-scheduler    100             500             12       WRR
mlag-class           3                mlag-scheduler          0               500             16       WRR
arp-ndp-class        4                arp-ndp-scheduler       100             500             32       WRR
lldp-class           5                lldp-scheduler          100             500             32       WRR
lacp-class           6                lacp-scheduler          100             500             32       WRR
bpdu-class           7                bpdu-scheduler          100             500             32       WRR
```

CoPP Configuration

- Configuration Notes
- Configuring CoPP
- Configuration Example

Configuration Notes

When configuring CoPP on a device, pay attention to the following points:

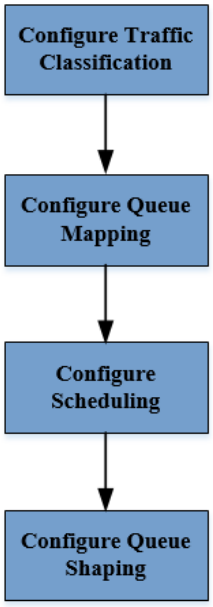
- CoPP configures control policy of the traffic from the ASIC to CPU. It is a very sensitive process of the whole switch OS. Any incorrect setting could impact the stability or could even paralyze the normal network operation. **It is therefore highly recommended to KEEP the default configurations of CoPP to ensure the system and network stability.**
- The CoPP policy takes effect only on the packets directed to the CPU.
- Users should not change the default sequence number of the system pre-defined control plane protocols. Please refer to Default Settings for CoPP for details about the pre-defined control plane protocols.
- For the current PicOS realization, IPv6 firewall filter rules are only supported on switch platforms of PRONTO3295, PRONTO3290, PRONTO3297 and AS4610_54P.
- The total value of min-bandwidth-pps of all activated queues should be less than CPU-affordable bandwidth, which should be the maximum bandwidth threshold to the CPU that is different depending on platform.
- Maximum of 32 CoPP matching rules specified with sequence number can be configured separately for IPv4 and IPv6 in the whole switch system.
- Users can change the pre-defined CoPP policies but are NOT allowed to delete them.
- It is acceptable that packets might be lost when users are making changes to the CoPP policies, such as when queue mapping is being set.
- The prerequisite of the protocol related CoPP policy taking effect is that the protocol function works well. BPDU, LLDP, LACP and ARP are not subject to this limitation.
- BPDU, LLDP, LACP and ARP cannot be classified through the protocol matching field, as they are not an IP protocol. You can classify these protocol packets through other matching fields, such as destination-mac-address, destination-port and ether-type.
- Adding IPv6 firewall filter rule could occupy as many as 128 TCAM ACL entries.
- The ranges of max-bandwidth-pps and min-bandwidth-pps are different on different platform.
- Although the realization and commands of CoPP use the QoS related module of CoS (Class of Service) and Firewall Filter Rule, but CoPP has its own command line with a fixed keyword **copp**, distinguishing it from the ACL feature.
- **set firewall filter copp sequence from protocol icmp** and **set firewall filter copp sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter copp sequence from protocol others** command with the protocol number.

Configuring CoPP

Figure 1 outlines the CoPP configuration process in the following steps:

1. Configure traffic classification: Define a group of matching rules to classify traffic which is the basis for differentiated services.
2. Configure queue mapping: Configure a forwarding class and local priority for sending different types of packets to a specified CPU queue.
3. Configure scheduling: Select a queue and process the packets from the queue with WRR scheduling algorithm and configure a queue scheduler weight.
4. Configure queue shaping: Set minimum bandwidth and maximum bandwidth for each CPU queue.

Figure 1 CoPP Configuration Process



Procedure

Step1 Configure CoPP firewall filter rule for traffic classification.

set firewall filter copp sequence <*number*> **from destination-mac-address** <*mac-address*>

NOTE:

- The matching fields of firewall filter rule could be **destination-mac-address**, **source-mac-address**, **destination-address-ipv4** for IPv4 matching rule, **destination-address-ipv6** for IPv6 matching rule, **source-address-ipv4** for IPv4 matching rule, **source-address-ipv6** for IPv6 matching rule, **protocol**, **destination-port**, **source-port**, **ether-type** and **vlan**.
- **and** is the logical operator between the matching fields with the same sequence number, that is, packets must match all of the matching fields with the same sequence number to be included in one class.
- Maximum of 32 CoPP matching rules specified with sequence number can be configured separately for IPv4 and IPv6 in the whole switch system.
- It is not allowed to commit the configuration if configured **from** node of matching field without configuring **then** node of the same sequence number. However, it is allowed to configure **then** node without configuring **from** node, the configuration of **then** node is not used.

Step2 Configure queue mapping of CoPP policy.

set firewall filter copp sequence <*number*> **then forwarding-class** <*forwarding-class name*>

Step3 Configure mapping between forwarding class and local priority.

set class-of-service forwarding-class <*forwarding-class-name*> **local-priority** <*int*>

Step4 Configure queue scheduler weight.

set class-of-service scheduler <*scheduler-name*> **weight** <*value*>

NOTE:

It is NOT recommended to use the weight value for CPU queue scheduling due to hardware restrictions.

Step5 Configure WRR scheduling algorithm for queue scheduling.

set class-of-service scheduler <*scheduler-name*> **mode WRR**

Step6 Configure max bandwidth and min bandwidth for queue shaping.

set class-of-service scheduler <*scheduler-name*> **max-bandwidth-pps** <*value*>

set class-of-service scheduler <*scheduler-name*> **min-bandwidth-pps** <*value*>

NOTE:

The total value of min-bandwidth-pps of all activated queues should be less than the CPU-affordable PPS depending on different platforms, which should be the maximum PPS threshold to the CPU.

Step7 Configure the DSCP remark for COPP.

set firewall filter copp sequence <*number*> **then dscp** <*dscp-value*>

Step8 Configure CoPP scheduler profile.

set class-of-service scheduler-profile copp-profile forwarding-class <*forwarding-class-name*> **scheduler** <*scheduler-name*>

Configuration Example

- Networking Requirements
- Procedure
- Verify the Configuration

Networking Requirements

In order to protect switch CPU from attacks and being overloaded by control plane packets, maintaining data forwarding and network topology stability, configure different CoPP policy for flows of different control plane protocols: SSH, NTP, TFTP and SLOW.

Procedure

Step1 Configure CoPP queue mapping, scheduling weight, scheduling algorithm and queue shaping.

```
admin@Xorplus# set class-of-service scheduler copp-scheduler180 mode WRR
admin@Xorplus# set class-of-service scheduler copp-scheduler180 max-bandwidth-pps 180
admin@Xorplus# set class-of-service scheduler copp-scheduler180 min-bandwidth-pps 0
admin@Xorplus# set class-of-service scheduler copp-scheduler180 weight 5
admin@Xorplus# set class-of-service scheduler-profile copp-profile forwarding-class copp-class1 scheduler copp-sche
admin@Xorplus# set class-of-service scheduler-profile copp-profile forwarding-class copp-class2 scheduler copp-sche

admin@Xorplus# set class-of-service scheduler copp-scheduler200 mode WRR
admin@Xorplus# set class-of-service scheduler copp-scheduler200 max-bandwidth-pps 200
admin@Xorplus# set class-of-service scheduler copp-scheduler200 min-bandwidth-pps 0
admin@Xorplus# set class-of-service scheduler copp-scheduler200 weight 10
admin@Xorplus# set class-of-service scheduler-profile copp-profile forwarding-class copp-class3 scheduler copp-sche

admin@Xorplus# set class-of-service scheduler copp-scheduler300 mode WRR
admin@Xorplus# set class-of-service scheduler copp-scheduler300 max-bandwidth-pps 300
admin@Xorplus# set class-of-service scheduler copp-scheduler300 min-bandwidth-pps 0
admin@Xorplus# set class-of-service scheduler copp-scheduler300 weight 20
admin@Xorplus# set class-of-service scheduler-profile copp-profile forwarding-class copp-class4 scheduler copp-sche
```

#Configure a policer 50pps.

```
admin@Xorplus# set firewall policer 50pps if-exceeding rate-limit 50
admin@Xorplus# set firewall policer 50pps if-exceeding burst-limit 50
```

#Configure mapping between forwarding class and local priority.

```
admin@Xorplus# set class-of-service forwarding-class copp-class1 local-priority 1
admin@Xorplus# set class-of-service forwarding-class copp-class2 local-priority 2
admin@Xorplus# set class-of-service forwarding-class copp-class3 local-priority 3
admin@Xorplus# set class-of-service forwarding-class copp-class4 local-priority 4
```

Step2 Configure destination-port and protocol to classify SSH flow, and mapping to forwarding class copp-class3.

```
admin@Xorplus# set firewall filter copp sequence 83 then action forward
admin@Xorplus# set firewall filter copp sequence 83 from destination-port 22
admin@Xorplus# set firewall filter copp sequence 83 from protocol tcp
admin@Xorplus# set firewall filter copp sequence 83 then forwarding-class copp-class3
admin@Xorplus# set firewall filter copp sequence 83 then policer 50pps

admin@Xorplus# set firewall filter copp sequence 84 then action forward
admin@Xorplus# set firewall filter copp sequence 84 from source-port 22
admin@Xorplus# set firewall filter copp sequence 84 from protocol tcp
admin@Xorplus# set firewall filter copp sequence 84 then forwarding-class copp-class3
admin@Xorplus# set firewall filter copp sequence 84 then policer 50pps
```

Step3 Configure destination-port, protocol and ether-type to classify NTP (Network Time Protocol) flow, and mapping to forwarding class copp-class1.

```
admin@Xorplus# set firewall filter copp sequence 91 then action forward
admin@Xorplus# set firewall filter copp sequence 91 from destination-port 123
```

```
admin@Xorplus# set firewall filter copp sequence 91 from protocol udp
admin@Xorplus# set firewall filter copp sequence 91 then forwarding-class copp-class1

admin@Xorplus# set firewall filter copp sequence 92 then action forward
admin@Xorplus# set firewall filter copp sequence 92 from destination-port 123
admin@Xorplus# set firewall filter copp sequence 92 from ether-type 34525
admin@Xorplus# set firewall filter copp sequence 92 from protocol udp
admin@Xorplus# set firewall filter copp sequence 92 then forwarding-class copp-class1
```

Step4 Configure destination-port, protocol and ether-type to classify TFTP flow, and mapping to forwarding class copp-class2.

```
admin@Xorplus# set firewall filter copp sequence 108 then action forward
admin@Xorplus# set firewall filter copp sequence 108 from destination-port 69
admin@Xorplus# set firewall filter copp sequence 108 from protocol udp
admin@Xorplus# set firewall filter copp sequence 108 then forwarding-class copp-class2

admin@Xorplus# set firewall filter copp sequence 109 then action forward
admin@Xorplus# set firewall filter copp sequence 109 from source-port 69
admin@Xorplus# set firewall filter copp sequence 109 from protocol udp
admin@Xorplus# set firewall filter copp sequence 109 then forwarding-class copp-class2
```

Step5 Configure destination-mac-address and ether-type to classify SLOW flow, and mapping to forwarding class copp-class4.

```
admin@Xorplus# set firewall filter copp sequence 111 then action forward
admin@Xorplus# set firewall filter copp sequence 111 from destination-mac-address 01:80:C2:00:00:02
admin@Xorplus# set firewall filter copp sequence 111 from ether-type 34825
admin@Xorplus# set firewall filter copp sequence 111 then forwarding-class copp-class4
```

Step6 Commit the configuration.

```
admin@XorPlus# commit
```

Verify the Configuration

- You can use the **run show copp bandwidth** command to view the bandwidth information, scheduling information and local priority of the forwarding class.

```
admin@Xorplus# run show copp bandwidth
Forwarding Class  Min-Bandwidth Max-Bandwidth Weight Local-Priority Schedule-Mode
default-class        0            100          24     0              WRR
copp-class1          0            180          5      1              WRR
copp-class2          0            180          5      2              WRR
copp-class3          0            200          10     3              WRR
copp-class4          0            300          20     4              WRR
pim-class            0            80           16     8              WRR
igmp-class           0            80           16     9              WRR
vrrp-class           0            80           16     10             WRR
dhcp-class           0            80           16     11             WRR
rip-class            0            80           16     12             WRR
ospf-class           0            80           16     13             WRR
bgp-class            0            80           16     14             WRR
mlag-mac-sync-class  0            80           16     15             WRR
mlag-class           0            80           16     16             WRR
bfd-class            0            80           16     17             WRR
arp-class            20           80           32     18             WRR
arp-class            20           80           32     19             WRR
lldp-class           20           80           32     20             WRR
lacp-class           20           80           32     21             WRR
bpdu-class           20           80           32     22             WRR
management-class     20           80           12     23             WRR
mvrp-class           100          500          32     24             WRR
erps-class           100          500          32     25             WRR
ripng-class          0            500          16     26             WRR
```

- You can use the **run show filter copp** command to view the configuration information of all CoPP policies, both pre-defined and user-defined, and match counter.

```
admin@Xorplus# run show filter copp
       Filter: copp
           Description:
```

```
Sequence: 10
    Description:
    match counter:  0 packets
    match-condition:
       protocol:                bpdu
    action: forward
    forwarding_class: bpdu-class
   ......
Sequence: 81
    Description:
    match counter:  0 packets
    match-condition:
       destination-port:        23..23
       protocol:                tcp
    action: forward
    forwarding_class: copp-class3
Sequence: 82
    Description:
    match counter:  0 packets
    match-condition:
       destination-port:        107..107
       protocol:                tcp
    action: forward
    forwarding_class: copp-class3
    policer: 50pps
Sequence: 83
    Description:
    match counter:  0 packets
    match-condition:
       destination-port:        22..22
       protocol:                tcp
    action: forward
    forwarding_class: copp-class3
    policer: 50pps
Sequence: 84
    Description:
    match counter:  0 packets
    match-condition:
       protocol:                tcp
       source-port:             22..22
    action: forward
    forwarding_class: copp-class3
    policer: 50pps
Sequence: 90
    Description:
    match counter:  0 packets
    match-condition:
       protocol:                dhcp
    action: forward
    forwarding_class: dhcp-class
Sequence: 91
    Description:
    match counter:  0 packets
    match-condition:
       destination-port:        123..123
       protocol:                udp
    action: forward
    forwarding_class: copp-class1
Sequence: 92
    Description:
    match counter:  0 packets
    match-condition:
       destination-port:        123..123
       ether-type:              0x86dd
       protocol:                udp
    action: forward
    forwarding_class: copp-class1
Sequence: 100
    Description:
    match counter:  0 packets
```

```
            match-condition:
               protocol:                vrrp
            action: forward
            forwarding_class: vrrp-class
        Sequence: 108
            Description:
            match counter:  0 packets
            match-condition:
               destination-port:        69..69
               protocol:                udp
            action: forward
            forwarding_class: copp-class2
        Sequence: 109
            Description:
            match counter:  0 packets
            match-condition:
               protocol:                udp
               source-port:             69..69
            action: forward
            forwarding_class: copp-class2
        Sequence: 110
            Description:
            match counter:  0 packets
            match-condition:
               protocol:                igmp
            action: forward
            forwarding_class: igmp-class
        Sequence: 111
            Description:
            match counter:  0 packets
            match-condition:
               destination-mac-address:  01:80:c2:00:00:02
               ether-type:              0x8809
            action: forward
            forwarding_class: copp-class4
        ......
    Input interface: inbound-control-plane
```

- You can use the **run show class-of-service interface inbound-control-plane** command to view the detail configuration information of CoPP profile.

```
admin@Xorplus# run show class-of-service interface inbound-control-plane
Interface : inbound-control-plane
Scheduler-profile : copp-profile
Forwarding-class     Local-priority   Scheduler               Min-Bandwidth   Max-Bandwidth   Weight   Schedule-Mo
------------------   --------------   ---------------------   -------------   -------------   ------   -----------
default-class        0                default-scheduler       0               80              8        WRR
pim-class            8                pim-scheduler           0               80              16       WRR
igmp-class           9                igmp-scheduler          0               80              16       WRR
vrrp-class           10               vrrp-scheduler          0               80              16       WRR
dhcp-class           11               dhcp-scheduler          0               80              16       WRR
rip-class            12               rip-scheduler           0               80              16       WRR
ospf-class           13               ospf-scheduler          0               80              16       WRR
bgp-class            14               bgp-scheduler           0               80              16       WRR
mlag-mac-sync-class  15               mlag-mac-sync-scheduler 0               80              16       WRR
mlag-class           16               mlag-scheduler          0               80              16       WRR
bfd-class            17               bfd-scheduler           0               80              16       WRR
ndp-class            18               arp-scheduler           20              80              32       WRR
arp-class            19               arp-scheduler           20              80              32       WRR
lldp-class           20               lldp-scheduler          20              80              32       WRR
lacp-class           21               lacp-scheduler          20              80              32       WRR
bpdu-class           22               bpdu-scheduler          20              80              32       WRR
management-class     23               management-scheduler    20              80              12       WRR
mvrp-class           24               mvrp-scheduler          20              80              32       WRR
erps-class           25               erps-scheduler          20              80              32       WRR
ripng-class          26               ripng-scheduler         0               80              16       WRR
```

- You can use the **run show copp statistics** command to view the statistics information of the forwarding class, including input and dropped packets and rate.

```
admin@Xorplus# run show copp statistics
```

```
All Copp Traffic statistics:
Input rate 272 bits/sec, 0 packets/sec
Input Packets.........................1
Input Octets..........................153
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0

arp-class Traffic statistics:
forwarding-class state: inactive
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets..........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0

copp-class1 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets..........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0

copp-class2 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets..........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0

copp-class3 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................106293
Input Octets..........................19345326
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0

copp-class4 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets..........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0
......
```

- You can use the **run show copp statistics active** command to view the statistics information of the forwarding class, state of which is active.

```
admin@Xorplus# run show copp statistics active
All Copp Traffic statistics:
Input rate 272 bits/sec, 0 packets/sec
Input Packets.........................1
Input Octets..........................153
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets..........................0


copp-class1 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
```

```
Input Octets.............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.............................0
Drop Octets..............................0

copp-class2 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets............................0
Input Octets.............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets............................0
Drop Octets.............................0

copp-class3 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets............................106293
Input Octets.............................19345326
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets............................0
Drop Octets.............................0

copp-class4 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets............................0
Input Octets.............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets............................0
Drop Octets.............................0
```

- You can use the **run show copp statistics forwarding-class** command to view the statistics information of the specified forwarding class.

```
admin@Xorplus# run show copp statistics forwarding-class copp-class1
copp-class1 Traffic statistics:

forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets............................0
Input Octets.............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets............................0
Drop Octets.............................0
```

- You can use the **run show interface stm** command to view the total STM resources that are available and how many STM entries are in use. The item **number of firewall egress tables** is used for describing STM resources of CoPP. By default, the value of **number of firewall egress tables** in **Stm resource in use:** is 21 as have been used by the default CoPP configurations.

```
admin@Xorplus# run show interface stm
Total stm resource:
  Share-mode: 5
  number of host routes: 32768
  number of mac unicast addresses: 32768
  number of firewall ingress tables: 896
  number of firewall egress tables: 510
  number of IPv4 unicast routes: 5000
  number of IPv6 unicast routes: 500
Stm resource in use:
  number of firewall ingress tables: 2
  number of firewall egress tables: 29
```

- You can use the **run clear copp statistics** command to clear the past statistics information of CoPP policy.

```
admin@Xorplus# run clear copp statistics
admin@Xorplus# commit
```

Default Settings for CoPP

- Default Queue Mapping Policy
- Default CLI Settings
- Show Default Settings of CoPP

NOTE:

- Default settings for CoPP in this page applies for all the PicOS supported switches except N2224PX-ON/N2248X-ON/N3208PX-ON.
- CoPP configures control policy of the traffic from the ASIC to CPU. It is a very sensitive process of the whole switch OS. Any incorrect setting could impact the stability or could even paralyze the normal network operation. **It is therefore highly recommended to KEEP the default configurations of CoPP to ensure the system and network stability.**

Default Queue Mapping Policy

By default, CoPP provides 27 CPU queues for data forwarding that would have a default scheduling weight. The system pre-defines 16 types of control plane protocols mapping from queue 8 to 26. The default queue mapping policy is as follows.

Table 1. Default Queue Mapping Policy

Protocols	CPU Queue	Default Scheduling Weight
MPLS LDP	29	16
IS-IS	28	16
Loopback Detection	27	32
RIPng	26	16
ERPS	25	32
MVRP	24	32
SSH/SNMP/NTP/TACACS/RADIUS	23	12
BPDU	22	32
LACP	21	32
LLDP	20	32
ARP	19	32
NDP	18	32
BFD	17	16
MLAG	16	16

MLAG-MAC-SYNC	15	16
BGP	14	16
OSPF	13	16
RIP	12	16
DHCP/DHCPv6	11	16
VRRP	10	16
IGMP	9	16
PIM	8	16
Reserved	7	-
Reserved	6	-
Reserved	5	-
Reserved	4	-
Reserved	3	-
Reserved	2	-
Reserved	1	-
Default*	0	0

Reserved: Reserved CPU queues indicate the CPU queues that have not been used by the system pre-defined queue mapping settings. For user-defined CoPP policy, it is recommended to use the reserved queues for queue mapping settings.

Default*: The flow of traffic directed to switch CPU will be sent to CPU queue 0 when the traffic matches no firewall filter rule.

But for the packet with an Inet Precedence or DSCP value, it will not always be sent to CPU queue 0 when the traffic matches no firewall filter rule. When you configure the classifier to classify services on different inbound interfaces by using **set class-of-service classifier trust-mode dscp** and **set class-of-service interface classifier** commands. The packets will be sent to the CPU queue according to the Inet Precedence or DSCP value. Mappings from Inet Precedence/DSCP value to CPU Queue are shown in the following tables.

Table 2. Mapping from Inet Precedence value to CPU Queue

Inet-precedence	CPU Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 3. Mapping from DSCP value to CPU Queue

DSCP	CPU Queue
0,1,2,3,4,5,6,7	0
8,9,10,11,12,13,14,15	1
16,17,18,19,20,21,22,23	2
24,25,26,27,28,29,30,31	3
32,33,34,35,36,37,38,39	4
40,41,42,43,44,45,46,47	5
48,49,50,51,52,53,54,55	6
56,57,58,59,60,61,62,63	7

Default CLI Settings

PicOS will startup with the following CLI commands by default. Users can change the pre-defined CoPP policies but are NOT allowed to delete them.

NOTE: The values of min-bandwidth-pps and max-bandwidth-pps are different on different platforms.

 # Default configurations of forwarding class for CoPP.

```
set class-of-service forwarding-class ldp-class local-priority 29
set class-of-service forwarding-class isis-class local-priority 28
set class-of-service forwarding-class loopback-detection-class local-priority 27
set class-of-service forwarding-class ripng-class local-priority 26
set class-of-service forwarding-class erps-class local-priority 25
set class-of-service forwarding-class mvrp-class local-priority 24
set class-of-service forwarding-class management-class local-priority 23
set class-of-service forwarding-class bpdu-class local-priority 22
set class-of-service forwarding-class lacp-class local-priority 21
set class-of-service forwarding-class lldp-class local-priority 20
set class-of-service forwarding-class arp-class local-priority 19
set class-of-service forwarding-class ndp-class local-priority 18
set class-of-service forwarding-class bfd-class local-priority 17
set class-of-service forwarding-class mlag-class local-priority 16
set class-of-service forwarding-class mlag-mac-sync-class local-priority 15
set class-of-service forwarding-class bgp-class local-priority 14
set class-of-service forwarding-class ospf-class local-priority 13
set class-of-service forwarding-class rip-class local-priority 12
set class-of-service forwarding-class dhcp-class local-priority 11
set class-of-service forwarding-class vrrp-class local-priority 10
set class-of-service forwarding-class igmp-class local-priority 9
set class-of-service forwarding-class pim-class local-priority 8
set class-of-service forwarding-class default-class local-priority 0
```

 # Default configurations of schedulers for CoPP.

```
set class-of-service scheduler ldp-scheduler mode WRR
set class-of-service scheduler ldp-scheduler weight 16
set class-of-service scheduler ldp-scheduler max-bandwidth-pps 80
set class-of-service scheduler ldp-scheduler min-bandwidth-pps 20

set class-of-service scheduler isis-scheduler mode WRR
set class-of-service scheduler isis-scheduler weight 16
set class-of-service scheduler isis-scheduler max-bandwidth-pps 80
set class-of-service scheduler isis-scheduler min-bandwidth-pps 20

set class-of-service scheduler loopback-detection-scheduler mode WRR
set class-of-service scheduler loopback-detection-scheduler weight 32
set class-of-service scheduler loopback-detection-scheduler max-bandwidth-pps 80
set class-of-service scheduler loopback-detection-scheduler min-bandwidth-pps 20

set class-of-service scheduler ripng-scheduler mode WRR
set class-of-service scheduler ripng-scheduler weight 16
set class-of-service scheduler ripng-scheduler max-bandwidth-pps 80
set class-of-service scheduler ripng-scheduler min-bandwidth-pps 0

set class-of-service scheduler erps-scheduler mode WRR
set class-of-service scheduler erps-scheduler weight 32
set class-of-service scheduler erps-scheduler max-bandwidth-pps 80
set class-of-service scheduler erps-scheduler min-bandwidth-pps 20

set class-of-service scheduler mvrp-scheduler mode WRR
set class-of-service scheduler mvrp-scheduler weight 32
set class-of-service scheduler mvrp-scheduler max-bandwidth-pps 80
set class-of-service scheduler mvrp-scheduler min-bandwidth-pps 20

set class-of-service scheduler management-scheduler mode WRR
set class-of-service scheduler management-scheduler weight 12
set class-of-service scheduler management-scheduler max-bandwidth-pps 80
set class-of-service scheduler management-scheduler min-bandwidth-pps 0

set class-of-service scheduler arp-scheduler mode WRR
set class-of-service scheduler arp-scheduler weight 32
set class-of-service scheduler arp-scheduler max-bandwidth-pps 80
set class-of-service scheduler arp-scheduler min-bandwidth-pps 0

set class-of-service scheduler ndp-scheduler mode WRR
set class-of-service scheduler ndp-scheduler weight 32
set class-of-service scheduler ndp-scheduler max-bandwidth-pps 80
set class-of-service scheduler ndp-scheduler min-bandwidth-pps 0

set class-of-service scheduler bfd-scheduler mode WRR
set class-of-service scheduler bfd-scheduler weight 16
set class-of-service scheduler bfd-scheduler max-bandwidth-pps 80
set class-of-service scheduler bfd-scheduler min-bandwidth-pps 20

set class-of-service scheduler mlag-scheduler mode WRR
set class-of-service scheduler mlag-scheduler weight 16
set class-of-service scheduler mlag-scheduler max-bandwidth-pps 80
set class-of-service scheduler mlag-scheduler min-bandwidth-pps 20

set class-of-service scheduler mlag-mac-sync-scheduler mode WRR
set class-of-service scheduler mlag-mac-sync-scheduler weight 16
set class-of-service scheduler mlag-mac-sync-scheduler max-bandwidth-pps 80
```

```
set class-of-service scheduler mlag-mac-sync-scheduler min-bandwidth-pps 20

set class-of-service scheduler bgp-scheduler mode WRR
set class-of-service scheduler bgp-scheduler weight 16
set class-of-service scheduler bgp-scheduler max-bandwidth-pps 80
set class-of-service scheduler bgp-scheduler min-bandwidth-pps 20

set class-of-service scheduler ospf-scheduler mode WRR
set class-of-service scheduler ospf-scheduler weight 16
set class-of-service scheduler ospf-scheduler max-bandwidth-pps 80
set class-of-service scheduler ospf-scheduler min-bandwidth-pps 20

set class-of-service scheduler rip-scheduler mode WRR
set class-of-service scheduler rip-scheduler weight 16
set class-of-service scheduler rip-scheduler max-bandwidth-pps 80
set class-of-service scheduler rip-scheduler min-bandwidth-pps 20

set class-of-service scheduler dhcp-scheduler mode WRR
set class-of-service scheduler dhcp-scheduler weight 16
set class-of-service scheduler dhcp-scheduler max-bandwidth-pps 80
set class-of-service scheduler dhcp-scheduler min-bandwidth-pps 20

set class-of-service scheduler vrrp-scheduler mode WRR
set class-of-service scheduler vrrp-scheduler weight 16
set class-of-service scheduler vrrp-scheduler max-bandwidth-pps 80
set class-of-service scheduler vrrp-scheduler min-bandwidth-pps 20

set class-of-service scheduler igmp-scheduler mode WRR
set class-of-service scheduler igmp-scheduler weight 16
set class-of-service scheduler igmp-scheduler max-bandwidth-pps 80
set class-of-service scheduler igmp-scheduler min-bandwidth-pps 20

set class-of-service scheduler pim-scheduler mode WRR
set class-of-service scheduler pim-scheduler weight 16
set class-of-service scheduler pim-scheduler max-bandwidth-pps 80
set class-of-service scheduler pim-scheduler min-bandwidth-pps 20

set class-of-service scheduler bpdu-scheduler mode WRR
set class-of-service scheduler bpdu-scheduler weight 32
set class-of-service scheduler bpdu-scheduler max-bandwidth-pps 80
set class-of-service scheduler bpdu-scheduler min-bandwidth-pps 20

set class-of-service scheduler lacp-scheduler mode WRR
set class-of-service scheduler lacp-scheduler weight 32
set class-of-service scheduler lacp-scheduler max-bandwidth-pps 80
set class-of-service scheduler lacp-scheduler min-bandwidth-pps 20

set class-of-service scheduler lldp-scheduler mode WRR
set class-of-service scheduler lldp-scheduler weight 32
set class-of-service scheduler lldp-scheduler max-bandwidth-pps 80
set class-of-service scheduler lldp-scheduler min-bandwidth-pps 20

set class-of-service scheduler default-scheduler mode WRR
set class-of-service scheduler default-scheduler weight 8
set class-of-service scheduler default-scheduler max-bandwidth-pps 80
set class-of-service scheduler default-scheduler min-bandwidth-pps 0

set class-of-service scheduler-profile copp-profile forwarding-class ldp-class scheduler ldp-scheduler
```

```
set class-of-service scheduler-profile copp-profile forwarding-class isis-class scheduler isis-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class loopback-detection-class scheduler loopback-detection-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class ripng-class scheduler ripng-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class erps-class scheduler erps-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class mvrp-class scheduler mvrp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class management-class scheduler management-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class bpdu-class scheduler bpdu-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class lacp-class scheduler lacp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class lldp-class scheduler lldp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class bfd-class scheduler bfd-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class mlag-class scheduler mlag-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class mlag-mac-sync-class scheduler mlag-mac-sync-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class bgp-class scheduler bgp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class ospf-class scheduler ospf-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class rip-class scheduler rip-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class dhcp-class scheduler dhcp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class vrrp-class scheduler vrrp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class igmp-class scheduler igmp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class pim-class scheduler pim-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class arp-class scheduler arp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class ndp-class scheduler ndp-scheduler
set class-of-service scheduler-profile copp-profile forwarding-class default-class scheduler default-scheduler
```

 # Apply schedulers of CoPP to inbound interface.

```
set class-of-service interface inbound-control-plane scheduler-profile copp-profile
```

 # Default configurations of protocol sequences and forwarding class.

```
set firewall filter copp sequence 10 from protocol bpdu
set firewall filter copp sequence 10 then forwarding-class bpdu-class
set firewall filter copp sequence 20 from protocol lacp
set firewall filter copp sequence 20 then forwarding-class lacp-class
set firewall filter copp sequence 30 from protocol lldp
set firewall filter copp sequence 30 then forwarding-class lldp-class
set firewall filter copp sequence 40 from protocol arp
set firewall filter copp sequence 40 then forwarding-class arp-class
set firewall filter copp sequence 50 from protocol ndp
set firewall filter copp sequence 50 then forwarding-class ndp-class
set firewall filter copp sequence 60 from protocol bfd
set firewall filter copp sequence 60 then forwarding-class bfd-class
set firewall filter copp sequence 70 from protocol mlag
set firewall filter copp sequence 70 then forwarding-class mlag-class
set firewall filter copp sequence 80 from protocol mlag-mac-sync
set firewall filter copp sequence 80 then forwarding-class mlag-mac-sync-class
set firewall filter copp sequence 90 from protocol bgp
set firewall filter copp sequence 90 then forwarding-class bgp-class
set firewall filter copp sequence 100 from protocol ospf
set firewall filter copp sequence 100 then forwarding-class ospf-class
set firewall filter copp sequence 110 from protocol rip
set firewall filter copp sequence 110 then forwarding-class rip-class
set firewall filter copp sequence 120 from protocol dhcp
```

```
set firewall filter copp sequence 120 then forwarding-class dhcp-class
set firewall filter copp sequence 130 from protocol vrrp
set firewall filter copp sequence 130 then forwarding-class vrrp-class
set firewall filter copp sequence 140 from protocol igmp
set firewall filter copp sequence 140 then forwarding-class igmp-class
set firewall filter copp sequence 150 from protocol pim
set firewall filter copp sequence 150 then forwarding-class pim-class
set firewall filter copp sequence 160 from protocol ssh
set firewall filter copp sequence 160 then forwarding-class management-class
set firewall filter copp sequence 170 from protocol snmp
set firewall filter copp sequence 170 then forwarding-class management-class
set firewall filter copp sequence 180 from protocol ntp
set firewall filter copp sequence 180 then forwarding-class management-class
set firewall filter copp sequence 190 from protocol tacacs
set firewall filter copp sequence 190 then forwarding-class management-class
set firewall filter copp sequence 200 from protocol radius
set firewall filter copp sequence 200 then forwarding-class management-class
set firewall filter copp sequence 210 from protocol mvrp
set firewall filter copp sequence 210 then forwarding-class mvrp-class
set firewall filter copp sequence 220 from protocol erps
set firewall filter copp sequence 220 then forwarding-class erps-class
set firewall filter copp sequence 230 from protocol ripng
set firewall filter copp sequence 230 then forwarding-class ripng-class
set firewall filter copp sequence 240 from protocol loopback-detection
set firewall filter copp sequence 240 then forwarding-class loopback-detection-class
set firewall filter copp sequence 250 from protocol ldp
set firewall filter copp sequence 250 then forwarding-class ldp-class
set firewall filter copp sequence 260 from protocol isis
set firewall filter copp sequence 260 then forwarding-class isis-class
set firewall filter copp sequence 270 from protocol dhcp6
set firewall filter copp sequence 270 then forwarding-class dhcp-class
```

#Apply firewall filter of CoPP to inbound interface.

```
set firewall filter copp input interface inbound-control-plane
```

Show Default Settings of CoPP

- You can use **run show copp bandwidth**, **run show class-of-service interface inbound-control-plane** and **run show filter copp** commands to view the default settings. (Besides default settings, the commands will also show the COPP configurations made by the user.)

```
admin@Xorplus# run show copp bandwidth
Forwarding Class           Min-Bandwidth Max-Bandwidth Weight Local-Priority Schedule-Mode
default-class              0             500           8      0              WRR
pim-class                  0             500           16     8              WRR
igmp-class                 0             500           16     9              WRR
vrrp-class                 0             500           16     10             WRR
dhcp-class                 0             500           16     11             WRR
rip-class                  0             500           16     12             WRR
ospf-class                 0             500           16     13             WRR
bgp-class                  0             500           16     14             WRR
mlag-mac-sync-class        0             500           16     15             WRR
mlag-class                 0             500           16     16             WRR
```

```
bfd-class                 0            500          16     17            WRR
ndp-class                 100          500          32     18            WRR
arp-class                 100          500          32     19            WRR
lldp-class                100          500          32     20            WRR
lacp-class                100          500          32     21            WRR
bpdu-class                100          500          32     22            WRR
management-class          100          500          12     23            WRR
mvrp-class                100          500          32     24            WRR
erps-class                100          500          32     25            WRR
ripng-class               0            500          16     26            WRR
loopback-detection-class  100          500          32     27            WRR
isis-class                0            500          16     28            WRR
```

```
admin@XorPlus#  run show filter copp
Filter: copp
    Description:
    Sequence: 10
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                bpdu
        action: forward
        forwarding_class: bpdu-class
    Sequence: 20
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                lacp
        action: forward
        forwarding_class: lacp-class
    Sequence: 30
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                lldp
        action: forward
        forwarding_class: lldp-class
    Sequence: 40
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                arp
        action: forward
        forwarding_class: arp-class
    Sequence: 50
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ndp
        action: forward
        forwarding_class: ndp-class
    Sequence: 60
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                bfd
        action: forward
```

```
        forwarding_class: bfd-class
    Sequence: 70
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                mlag
        action: forward
        forwarding_class: mlag-class
    Sequence: 80
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                mlag-mac-sync
        action: forward
        forwarding_class: mlag-mac-sync-class
    Sequence: 90
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                bgp
        action: forward
        forwarding_class: bgp-class
    Sequence: 100
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ospf
        action: forward
        forwarding_class: ospf-class
    Sequence: 110
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                rip
        action: forward
        forwarding_class: rip-class
    Sequence: 120
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                dhcp
        action: forward
        forwarding_class: dhcp-class
    Sequence: 130
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                vrrp
        action: forward
        forwarding_class: vrrp-class
    Sequence: 140
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                igmp
        action: forward
        forwarding_class: igmp-class
    Sequence: 150
```

```
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                pim
        action: forward
        forwarding_class: pim-class
    Sequence: 160
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ssh
        action: forward
        forwarding_class: management-class
    Sequence: 170
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                snmp
        action: forward
        forwarding_class: management-class
    Sequence: 180
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                ntp
        action: forward
        forwarding_class: management-class
    Sequence: 190
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                tacacs
        action: forward
        forwarding_class: management-class
    Sequence: 200
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                radius
        action: forward
        forwarding_class: management-class
    Sequence: 210
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                mvrp
        action: forward
        forwarding_class: mvrp-class
    Sequence: 220
        Description:
        match counter:  69379 packets
        match-condition:
            protocol:                erps
        action: forward
        forwarding_class: erps-class
    Sequence: 230
        Description:
        match counter:  0 packets
```

```
        match-condition:
            protocol:                ripng
        action: forward
        forwarding_class: ripng-class
    Sequence: 240
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                loopback-detection
        action: forward
        forwarding_class: loopback-detection-class
    Sequence: 250
        Description:
        match counter: 0 packets
        match-condition:
            protocol: ldp
        action: forward
        forwarding_class: ldp-class
    Sequence: 260
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                isis
        action: forward
        forwarding_class: isis-class
    Sequence: 270
        Description:
        match counter:  0 packets
        match-condition:
            protocol:                dhcp6
        action: forward
        forwarding_class: dhcp-class
  Input interface: inbound-control-plane
```

```
admin@Xorplus#  run show class-of-service interface inbound-control-plane
Interface : inbound-control-plane
Scheduler-profile : copp-profile
Forwarding-class     Local-priority   Scheduler               Min-Bandwidth   Max-Bandwidth   Weight          Schedule-Mode
------------------   --------------   ---------------------   -------------   -------------   ------   -------------
default-class        0                default-scheduler       0               80              8        WRR
pim-class            8                pim-scheduler           0               80              16       WRR
igmp-class           9                igmp-scheduler          0               80              16       WRR
vrrp-class           10               vrrp-scheduler          0               80              16       WRR
dhcp-class           11               dhcp-scheduler          0               80              16       WRR
rip-class            12               rip-scheduler           0               80              16       WRR
ospf-class           13               ospf-scheduler          0               80              16       WRR
bgp-class            14               bgp-scheduler           0               80              16       WRR
mlag-mac-sync-class  15               mlag-mac-sync-scheduler 0               80              16       WRR
mlag-class           16               mlag-scheduler          0               80              16       WRR
bfd-class            17               bfd-scheduler           0               80              16       WRR
ndp-class            18               ndp-scheduler           20              80              32       WRR
arp-class            19               arp-scheduler           20              80              32       WRR
lldp-class           20               lldp-scheduler          20              80              32       WRR
lacp-class           21               lacp-scheduler          20              80              32       WRR
bpdu-class           22               bpdu-scheduler          20              80              32       WRR
```

```
management-class     23              management-scheduler    20              80              12       WRR
mvrp-class           24              mvrp-scheduler       20              80              32       WRR
erps-class           25              erps-scheduler       20              80              32       WRR
ripng-class          26              ripng-scheduler         0               80              16       WRR
loopback-detection-class 27          loopback-detection-scheduler 100        500             32       WRR
isis-class           28              isis-scheduler          0               500             16       WRR
ldp-class            29              ldp-scheduler           0               500             16       WRR
```

Queue-based Rate Limiting

- Configuring Queue-based Rate Limiting
  - Procedure
- Configuration Example
  - Network Requirements
  - Procedure

The queue-based rate limiting controls the rate of the physical interface egress queue to adjust the traffic rates to enable traffic to be transmitted at an even rate, thus preventing congestion on the downstream device. When the transmit rate of packets exceeds the queue-based rate limit, the packets will be discarded.

Configuring Queue-based Rate Limiting

When packets arrive, the system classifies packets and places them into different egress queues. The device can provide differentiated services for queues of different priorities using different rate limiting parameter settings for these queues.

Procedure

Step1 Configure scheduling algorithm for queue scheduling.

set class-of-service scheduler <*scheduler-name*> **mode** <**SP | WRR | WFQ**>

Step2 Configure guaranteed rate and the maximum rate for the interface queue.

set class-of-service scheduler <*scheduler-name*> **guaranteed-rate** <*value*>

set class-of-service scheduler <*scheduler-name*> **max-rate** <*value*>

> **NOTE:**
>
> If both queue-based rate limiting and interface-based rate limiting (configured by the command **set interface gigabit-ethernet** <*port*> **rate-limiting** <**ingress** | **egress**> **kilobits** <*kilobits-ps*>) are configured on the interface, the smaller value of the two will be used for rate limiting.

Step3 Configure scheduler profile associated with the configured scheduler and forwarding class.

set class-of-service scheduler-profile <*scheduler-profile-name*> **forwarding-class** <*forwarding-class-name*> **scheduler** <*scheduler-name*>

Step4 Configure mapping between forwarding class and local priority.

set class-of-service forwarding-class <*forwarding-class-name*> **local-priority** <*int*>

Step5 Apply the scheduler profile to an egress interface.

set class-of-service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>

Configuration Example

Network Requirements

As shown in Figure 1, User1, User2, and User3 are three different types of user devices in the network. They are respectively connected to the interfaces Ge-1/1/1, Ge-1/1/2, and Ge-1/1/3 of the Switch. The Switch is connected to the Router through interface Ge-1/1/4.

On the Switch, configure service classification for different users and queue mapping of egress interface for different services. Set different guaranteed rate and maximum rate for the physical interface egress queues for different services to reduce network congestion and ensure the bandwidth requirements of each service.

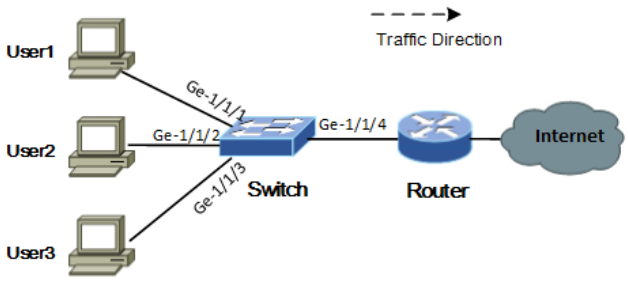


Figure 1. Queue-based Rate Limiting Configuration Example

The configuration process is as follows:

1. Create VLANs and configure VLAN members on each interface to enable the users to access the network through the Switch.
2. Configure classifier to classify services on different inbound interfaces and queue mapping of outbound interface for different services.
3. Configure queue schedulers for the physical interface egress queue.
4. Configure queue-based rate limiting to limit the bandwidth of User1, User2, and User3 services.

Procedure

Step1 Configure VLANs.

```
admin@XorPlus# set vlans vlan-id 199
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 199
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 199
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 199
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching vlan members 199
```

Step2 Configure classifier to classify services on different inbound interfaces.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c2 trust-mode inet-precedence
admin@XorPlus# set class-of-service classifier c3 trust-mode dscp
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# set class-of-service interface ge-1/1/2 classifier c2
admin@XorPlus# set class-of-service interface ge-1/1/3 classifier c3
```

Step3 Configuring the queue scheduling algorithm.

```
admin@XorPlus# set class-of-service scheduler s1 mode SP
admin@XorPlus# set class-of-service scheduler s2 mode SP
admin@XorPlus# set class-of-service scheduler s3 mode SP
```

Step4 Configure the guaranteed rate and maximum rate of the interface egress queue.

```
admin@XorPlus# set class-of-service scheduler s1 guaranteed-rate 5000
admin@XorPlus# set class-of-service scheduler s2 guaranteed-rate 15000
admin@XorPlus# set class-of-service scheduler s3 guaranteed-rate 20000
admin@XorPlus# set class-of-service scheduler s1 max-rate 30000
admin@XorPlus# set class-of-service scheduler s2 max-rate 30000
admin@XorPlus# set class-of-service scheduler s3 max-rate 30000
```

Step5 Configure the scheduler-profile and queue mapping of egress interface.

```
admin@XorPlus# set class-of-service forwarding-class f0 local-priority 0
admin@XorPlus# set class-of-service forwarding-class f3 local-priority 3
admin@XorPlus# set class-of-service forwarding-class f7 local-priority 7
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f0 scheduler s1
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f3 scheduler s2
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f7 scheduler s3
```

Step6 Apply scheduler-profile to egress interface Ge-1/1/4.

```
admin@XorPlus# set class-of-service interface ge-1/1/4 scheduler-profile p1
```

Interface-based Rate Limiting

Interface-based rate limiting controls the total rate of all packets passing through an interface to ensure that the bandwidth usage is within the allowed range. For the same interface, you can configure interface-based rate limiting in both ingress and egress directions or in only one direction.

- Configuring Ingress Interface-based Rate Limiting
- Configuring Egress Interface-based Rate Limiting

Configuring Ingress Interface-based Rate Limiting

If you do not limit the traffic sent by users, the continuous burst of data of a large number of users will make the network more crowded. By configuring the ingress interface-based rate limiting on the interface, you can limit the traffic entering the interface to a reasonable range.

set interface gigabit-ethernet <*interface-name*> **rate-limiting ingress kilobits** <*value*>

set interface gigabit-ethernet <*interface-name*> **rate-limiting ingress ratio** <*value*>

set interface gigabit-ethernet <*interface-name*> **rate-limiting ingress burst** <*burst-size*>

NOTE:

- In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
- Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.
- When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** <*interface-name*> **rate-limiting ingress kilobits** <*value*> or **set interface gigabit-ethernet** <*interface-name*> **rate-limiting ingress ratio** <*value*> command.

Configuration Example

- Set the rate limit to 8000 kbit/s on interface te-1/1/1 for the ingress traffic, and use the system adapted burst size.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 rate-limiting ingress kilobits 8000
admin@Xorplus# commit
```

- You can use **run show interface gigabit-ethernet** command to check the configuration, where "**Interface rate limit ingress: , egress:** " and "**Interface burst limit ingress: , egress:** " indicating the configuration of interface-based rate limit and burst size.

```
admin@Xorplus# run show interface gigabit-ethernet te-1/1/1
Physical interface: te-1/1/1, Enabled, error-discard False, Physical link is Down
Interface index: 1, Mac Learning Enabled
Port mode:  access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:8000kbps, egress:unlimited
Interface burst limit ingress:10kb, egress:unlimited
Link fault signaling ignore local fault:false, ignore remote fault:false
force up mode:false
Precision Time Protocol mode:none
Current address: cc:37:ab:b6:9b:55, Hardware address: cc:37:ab:b6:9b:55
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Output Packets............................0
Input Octets..............................0
Output Octets............................0
```

Configuring Egress Interface-based Rate Limiting

To control the rate of all outgoing traffic on an interface, configure egress interface-based rate limiting. When the transmit rate of packets exceeds the configured rate limit, the excess packets will be discarded.

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress kilobits** <*value*>

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress ratio** <*value*>

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress burst** <*burst-size*>

> **NOTE**:
>
> - In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
> - When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress kilobits** <*value*> or **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress ratio** <*value*> command.

Configuration Example

- Set the rate limit to 8000 kbit/s on interface te-1/1/1 for the egress traffic, and use the system adapted burst size.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 rate-limiting egress kilobits 8000
admin@Xorplus# commit
```

- You can use **run show interface gigabit-ethernet** command to check the configuration, where "**Interface rate limit ingress: , egress:** " and "**Interface burst limit ingress: , egress:** " indicating the configuration of interface-based rate limit and burst size.

```
admin@Xorplus# run show interface gigabit-ethernet te-1/1/1
Physical interface: xe-1/1/1(49), Enabled, error-discard False, Physical link is Down
Interface index: 73, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1518, Speed: Auto, Duplex: Full
Cdr: Enabled
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Disabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit  ingress: unlimited, egress: unlimited
Interface burst limit ingress: unlimited, egress: unlimited
Link fault signaling  ignore local fault: false, ignore remote fault: false
Force up mode: false
Precision Time Protocol mode: none
Current address: 0c:81:3e:5c:00:00, Hardware address: 0c:81:3e:5c:00:00
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.....................0
  Output Packets.....................0
  Input Octets.....................0
  Output Octets.....................0
```

WRR Configuration Example

As shown in Fig 2, ge-1/1/1 and ge-1/1/2 are ingress ports. ge-1/1/3 is the egress port. Use WRR scheduling model: priority trust mode is IEEE 802.1.

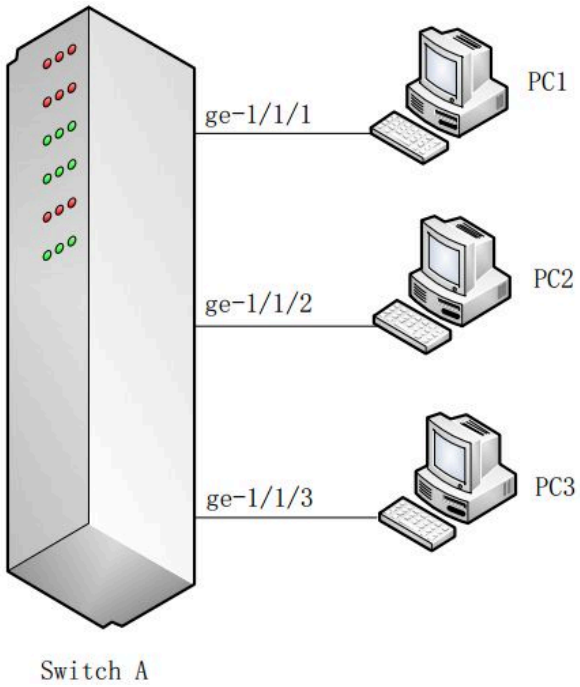


Fig 2. Configure WRR

Configure Scheduler

Configure two schedulers: s1 and s2. Their modes are WRR. Configure scheduler s1's weight as 1 and s2's weight as 3.

```
admin@XorPlus# set class-of-service scheduler s1 mode WRR
admin@XorPlus# set class-of-service scheduler s2 mode WRR
admin@XorPlus# set class-of-service scheduler s1 weight 1
admin@XorPlus# set class-of-service scheduler s2 weight 3
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Two Forwarding-Classes

Configure forwarding-classes, f1, f2, and their local-priorities.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 3
admin@XorPlus# set class-of-service forwarding-class f2 local-priority 6
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Classifiers and Apply Classifiers to Ingress Ports

Configure classifier c1, c2, and the trust mode for each. Configure classifier relevant to the forwarding class. Both c1 and c2 are used as ingress ports, and they should contain code point, not scheduler.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 5
admin@XorPlus# set class-of-service classifier c2 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c2 forwarding-class f2 code-point 7
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# set class-of-service interface ge-1/1/2 classifier c2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                     0
1                SP,0kbps                     1
2                SP,0kbps                     2
3                SP,0kbps                     3,5
4                SP,0kbps                     4
5                SP,0kbps
6                SP,0kbps                     6
7                SP,0kbps                     7
admin@XorPlus# run show class-of-service interface ge-1/1/2
Interface : ge-1/1/2
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                     0
1                SP,0kbps                     1
2                SP,0kbps                     2
3                SP,0kbps                     3
4                SP,0kbps                     4
5                SP,0kbps                     5
6                SP,0kbps                     6,7
7                SP,0kbps
```

Configuring Scheduler Profile and Apply Scheduler Profile to Egress Ports

Scheduler profile p1 is used for egress port ge-1/1/3 and should contain a scheduler not containing code point.

```
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f1 scheduler s1
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f2 scheduler s2
admin@XorPlus# commit
Commit OK.
```

```
Save done.
admin@XorPlus# set class-of-service interface ge-1/1/3 scheduler-profile p1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/3
Interface : ge-1/1/3
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                    Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                WRR,1,0kbps
4                SP,0kbps
5                SP,0kbps
6                WRR,3,0kbps
7                SP,0kbps
```

Generate Traffic

PC1 and PC2 generate traffic that are matched with the corresponding classifier. PC1 and PC2 send 100% of traffic to PC3 at the same time.

The expected result is that PC3 can receive packets from PC1 and PC2, and their rate is 1:3, that is the weight proportion in the corresponding queue.

Buffer Management

NOTE:

On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.

Introduction

When the network congestion, the port don't send data immediately, to prevent data loss, device can transmit the temporay storage of data to the data buffer.

1. Accounting Resources

The chip has the fixed-sized cells. Each cell is 208 bytes long. The first cell used by a packet contains two payloads. The first payload is a 64-byte packet descriptor, and the second payload contains 144 bytes of packet data. Every cell, after the first one used by a packet, uses the complete 208 bytes for packet data . A packet use at least one cell. The length of packet decides how many cell the packet uses. For example， untagged packeets 64 bytes to 144 bytes long use one cell. A 352-byte packet would require two cells. And packets from 1393-bytes to 1600-bytes long use eight cells.

2. Memory Spaces

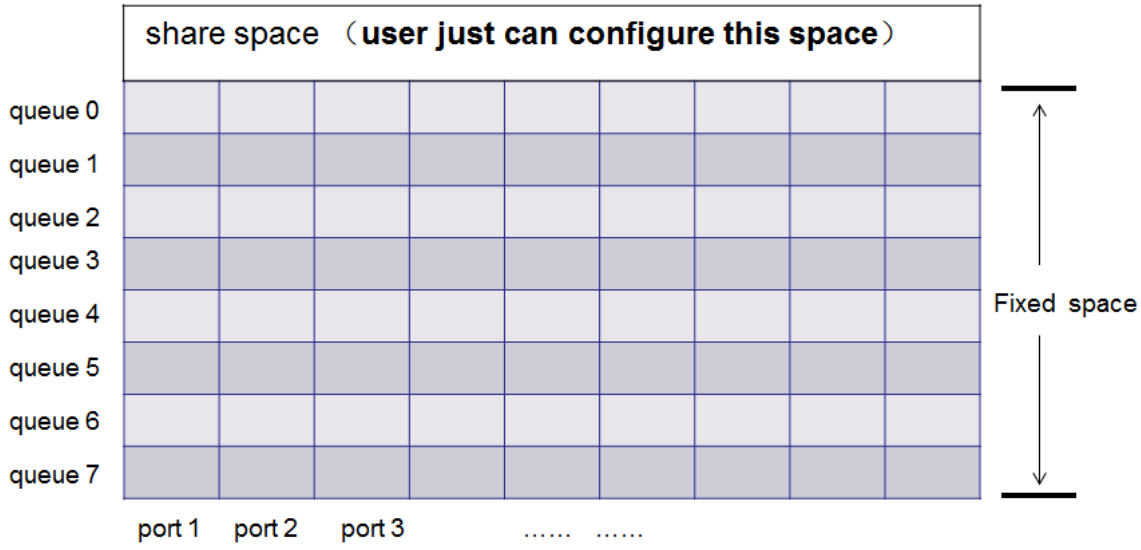
The cell data buffer is divided into fixed and shared spaces.

- Fixed space

Fixed space provide minimum guaranteed space on a per priority group and per port basis. This space cannot be shared with other ports. When the port congestion occurs, it will occupy fixed space first, shared space will be used when the fixed space is full. The Fixed space should not be too big, otherwise it will waste space resources.

- Shared space

The shared space will be used by all ports and priority groups when the fixed space run out. When the shared space is used up, the packet is discarded. If a queue don't store packet, the others queue will grab this queue space. For a queue,all of ports transmit packets will first come first served, if the used resource reach the threhold, packets will be dropped after arrived.The shared space can be configured dynamic or static threshold at the logical level of the queue.



Command configuration

The device provide separate UC (unicast) and MC (multicase) queue. For the unicast queue and multicast queue. The UC queues are used to store known unicast packets and can be flexibly assigned while the MC queues are used to store DLF, multicast, broadcast and mirrored packets. While the CPU port does not support separate UC and MC queues, the CPU port does have a total of 48 queues available, and these queues are eligible for both UC and MC traffic based on CPU Cos mapping. We have different configuration to deal with share space：

1.multicast queue：

static mode: This is the default configuration

- The value of the static threshold is configured for the multicast queue in the shared space.This avoids the case that the port enabled flow control or PFC affects the forwarding of other ports. But the disadvantage is less efficient use of memory.

dynamic mode : Need to configure

- The memory threhold is adjusted dynamically according to the avaliable shared memory in this mode. The threholds will reduce when the remaining shared memory reduces. The threholds will rise up when the remaining shared memory rises up.

For example, enable queue 0 dynamic-shared

```
root@XorPlus# set interface ethernet-switching-options buffer egress-queue 0 mc-queue-dynamic-shared true
root@XorPlus# commit
Commit OK.
Save done.
```

2.unicast queue：

dynamic mode ：

- dynamic threshold is the default mode for the unicast queue，and it can't configure static threshold.

3.dynamic threshold ratio configuration

The dynamic mode both of multicast (must enable dynamic threshold) and unicast queue can configure the max dynamic threshold ratio. The threhold is still dynamically adjusted until reaching the max ratio configured.

For example, configure dynamic threshold ratio 50% for queue 0

```
root@XorPlus# set interface ethernet-switching-options buffer egress-queue 0 shared-ratio 50
root@XorPlus# commit
```

Check the configuration result

```
root@XorPlus# run show interface egress-buffer
Queue UC-Enabled UC-Shared-Ratio MC-Enabled MC-Shared-Ratio
0     true       50              true       50
1     true       33              false      --
2     true       33              false      --
3     true       33              false      --
4     true       33              false      --
5     true       33              false      --
6     true       33              false      --
7     true       33              false      --
```

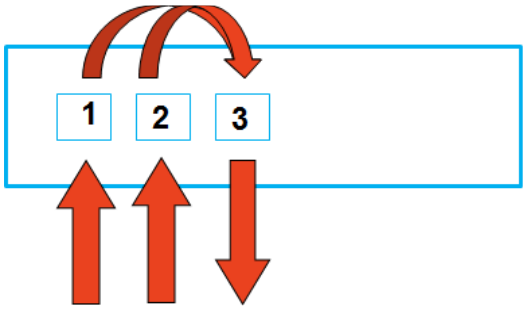
For the maximum shared-area ratio for a queue, the percentage values 0 to 100 are divided into 10 rages.The table below shows the effective values that correspond to the configured values of ratio-value.

Value of *ratio-value*	Effective value
0 to 1	1
2 to 3	3
4 to 7	6
8 to 16	11
17 to 29	20
30 to 42	33
43 to 60	50
61 to 76	67
77 to 86	80
87 to 100	89

notice

Now, multicast queue just support eight （1~67）effective ratio value on all platforms

Application notice



As show above: send packets from port1 and port2 to port3 in 10G speed in queue 0, and port3 will be in congestion.

For the multicast flow, if flow control is enabled on port1 and port2 and configure static threshold, the packets also perhaps will be dropped in port 3 egress queue. Ingress don't send pause frame because egress's shared-ratio is smaller than ingress's and egress reach it's threhold before igress reach.

So if users meet this issue, in this case, we suggest users configure dynamic mode. port1 and port2 will send out pause frame before port3 queue limit is reached, and accept burst packets to avoid packet drop.

WFQ Configuration Example

As shown in Fig 3, ge-1/1/1 and ge-1/1/2 are ingress ports. ge-1/1/3 is the egress port. Use the WFQ scheduling model. Priority trust model is IEEE 802.1. The bandwidth is 100Mbps.

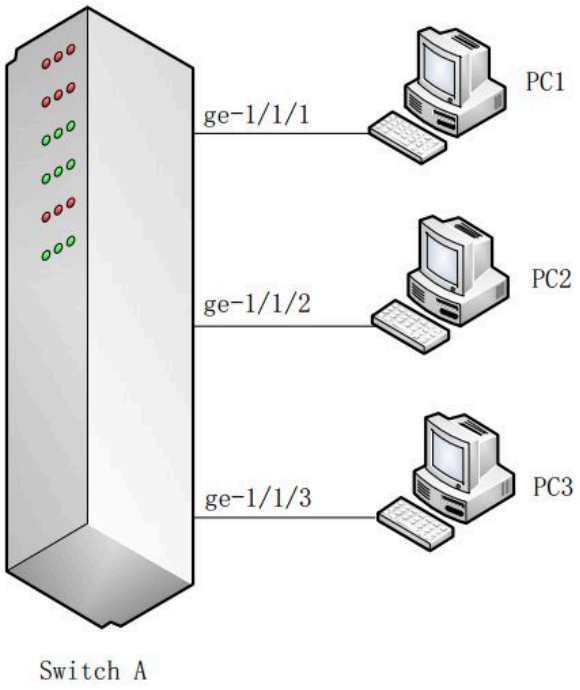


Fig 3. Configure WFQ

Configure Scheduler

Configure two schedulers (s1 and s2) with guaranteed-rates and their modes WFQ. Configure scheduler s1 weighted at 1 and scheduler s2 weighted at 3. The guaranteed-rate of scheduler s1 is 10000, and the guaranteed-rate of scheduler s2 is 30000.

```
admin@XorPlus# set class-of-service scheduler s1 mode WFQ
admin@XorPlus# set class-of-service scheduler s2 mode WFQ
admin@XorPlus# set class-of-service scheduler s1 weight 1
admin@XorPlus# set class-of-service scheduler s1 guaranteed-rate 10000
admin@XorPlus# set class-of-service scheduler s2 weight 3
admin@XorPlus# set class-of-service scheduler s2 guaranteed-rate 30000
admin@XorPlus# commit
Commit OK.
Save done.
```

Configure Two Forwarding-Classes

Configure forwarding-class f1 and f2 and their local-priorities.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 3
admin@XorPlus# set class-of-service forwarding-class f2 local-priority 6
```

```
admin@XorPlus# commit
Commit OK.
Save done.
```

Configuring Classifier and Apply Classifiers to Ingress Ports

Configure classifier c1, c2, and c3, as well as the trust mode. Configure classifiers relevant to the forwarding class. Classifiers c1 and c2 are used as the ingress ports, and they should contain code point, not scheduler.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 5
admin@XorPlus# set class-of-service classifier c2 trust-mode ieee-802.1
admin@XorPlus# set class-of-service classifier c2 forwarding-class f2 code-point 7
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# set class-of-service interface ge-1/1/2 classifier c2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                      0
1                SP,0kbps                      1
2                SP,0kbps                      2
3                SP,0kbps                      3,5
4                SP,0kbps                      4
5                SP,0kbps
6                SP,0kbps                      6
7                SP,0kbps                      7
admin@XorPlus# run show class-of-service interface ge-1/1/2
Interface : ge-1/1/2

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                      0
1                SP,0kbps                      1
2                SP,0kbps                      2
3                SP,0kbps                      3
4                SP,0kbps                      4
5                SP,0kbps                      5
6                SP,0kbps                      6,7
7                SP,0kbps
```

Configuring Scheduler Profile and Apply Classifiers to Egress Ports

Scheduler profile p1 is used to egress port ge-1/1/3 and should contain a scheduler not containing code point.

```
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f1 scheduler s1
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f2 scheduler s2
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set class-of-service interface ge-1/1/3 scheduler-profile p1
admin@XorPlus# commit
Commit OK.
Save done.

admin@XorPlus# run show class-of-service interface ge-1/1/3
Interface : ge-1/1/3

trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                WFQ,1,10000kbps
4                SP,0kbps
5                SP,0kbps
6                WFQ,3,30000kbps
7                SP,0kbps
```

Generate Traffic

PC1 and PC2 generate traffic which are matched with the corresponding classifier. PC1 and PC2 send 100% traffic to PC3 at the same time.

The expected result is that PC3 can receive packets from PC1 and PC2, and their rate is about 1:3. That is, the weight proportion and the guaranteed-rate have corresponding queues.

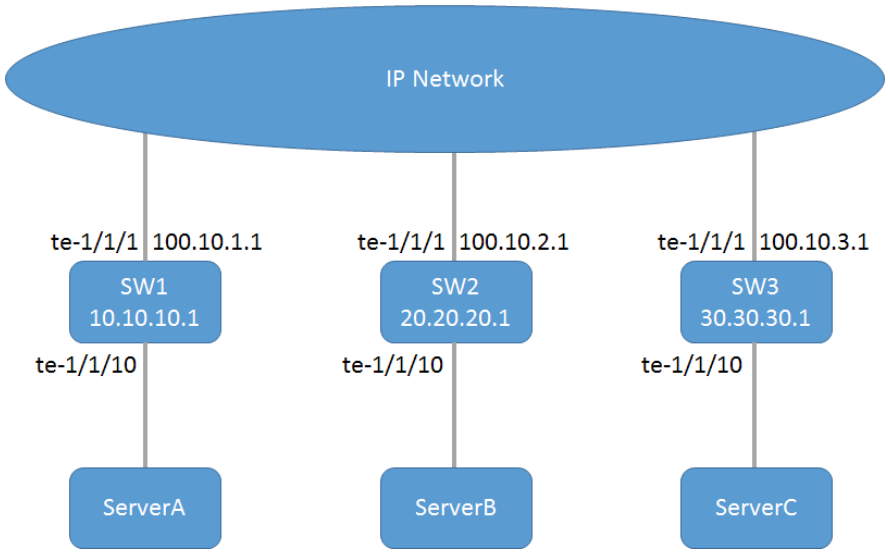
VXLAN Configuration

- VXLAN Base Configuration Example
- VXLAN Routing
  - Cross-Subnet Packet Forwarding Process
  - Example for Configuring VXLAN for Different Subnets
- VXLAN Configuration Guide
- VXLAN ECMP Configuration

VXLAN Base Configuration Example

> **NOTE:**
> Enable IP routing function before using this feature, for details please refer to Configuring IP Routing.

Topology



SW1 Configure

```
set vlans vlan-id 10
set vlans vlan-id 2000 l3-interface vlan2000
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2000
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
set l3-interface loopback lo address 10.10.10.1 prefix-length 32
set l3-interface vlan-interface vlan2000 address 100.10.1.1 prefix-length 24
set protocols static route 20.20.20.1/32 next-hop 100.10.1.2
set protocols static route 30.30.30.1/32 next-hop 100.10.1.2
set vxlans source-interface lo address 10.10.10.1
set vxlans vni 1000 flood vtep 20.20.20.1
set vxlans vni 1000 flood vtep 30.30.30.1
set vxlans vni 1000 vlan 10
set vxlans vni 1000 decapsulation mode none
set vxlans vni 1000 encapsulation mode none
set ip routing enable true
```

SW2 Configure

```
set vlans vlan-id 10
set vlans vlan-id 2000 l3-interface vlan2000
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2000
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
set l3-interface loopback lo address 20.20.20.1 prefix-length 32
set l3-interface vlan-interface vlan2000 address 100.10.2.1 prefix-length 24
set protocols static route 10.10.10.1/32 next-hop 100.10.2.2
set protocols static route 30.30.30.1/32 next-hop 100.10.2.2
set vxlans source-interface lo address 20.20.20.1
set vxlans vni 1000 flood vtep 10.10.10.1
set vxlans vni 1000 vlan 10
set vxlans vni 1000 decapsulation mode none
set vxlans vni 1000 encapsulation mode none
set ip routing enable true
```

SW3 Configure

```
set vlans vlan-id 10
set vlans vlan-id 2000 l3-interface vlan2000
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2000
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
```

```
set l3-interface loopback lo address 30.30.30.1 prefix-length 32
set l3-interface vlan-interface vlan2000 address 100.10.3.1 prefix-length 24
set protocols static route 10.10.10.1/32 next-hop 100.10.3.2
set protocols static route 20.20.20.1/32 next-hop 100.10.3.2
set vxlans source-interface lo address 30.30.30.1
set vxlans vni 1000 flood vtep 10.10.10.1
set vxlans vni 1000 vlan 10
set vxlans vni 1000 decapsulation mode none
set vxlans vni 1000 encapsulation mode none
set ip routing enable true
```

VXLAN Routing

This section provides how to implement and deploy VXLAN routing for L3 routing.

- Cross-Subnet Packet Forwarding Process
- Example for Configuring VXLAN for Different Subnets

Cross-Subnet Packet Forwarding Process

Cross-subnet packet forwarding between VXLAN and VXLAN subnet or between VXLAN and non-VXLAN subnet can be implemented through a Layer 3 gateway.

Supported Platforms

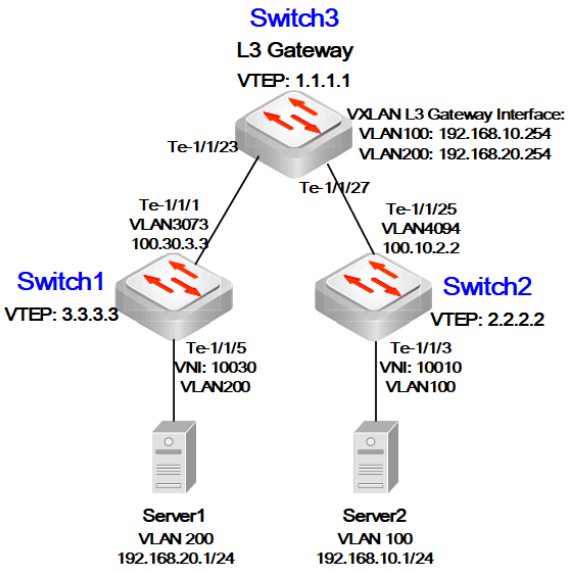
- VXLAN routing is supported on the following ASIC platforms: Trident2+, Trident3-X7, Trident3-X5 (Maverick2) and Trident3-X3 (Helix5).
- For Trident2+ switches, VXLAN routing can not work with non-VXLAN interface (including CPU interface). For example, it is not supported to forward a decapsulated VXLAN packet through a non-VXLAN port (for this example, users can configure the non-VXLAN interface to a VXLAN interface to solve the problem).

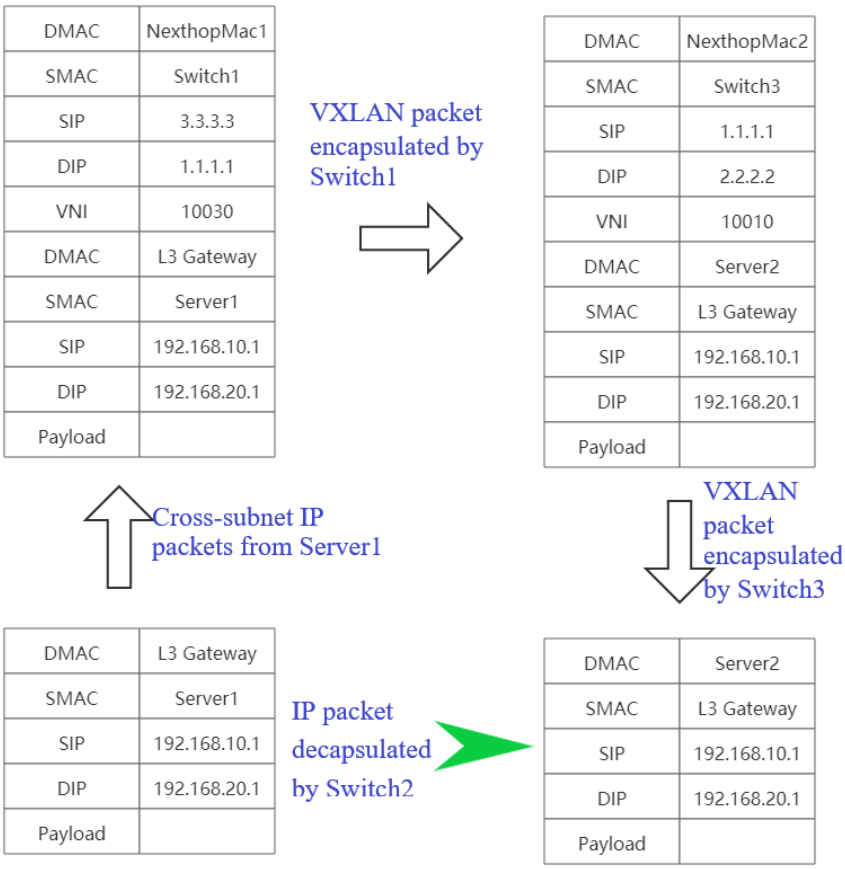
Cross-Subnet Packet Forwarding Process

PicOS supports to apply VXLAN routing on centralized gateway and distributed gateway.

Figure 1 shows the topology of cross-subnet packet forwarding and packet encapsulation in the centralized gateway scenario. A centralized gateway is a Layer 3 gateway deployed centrally on a single device, where all cross-subnet traffic is forwarded through the Layer 3 gateway to achieve centralized management of traffic.

Figure 1 Topology of cross-subnet packet forwarding and packet encapsulation





The packet forwarding process is as follows:

1. Switch 1 receives the message from Server 1, obtains the corresponding layer 2 broadcast domain according to the access port and VLAN information in the message, and finds out the interface and encapsulation information in the corresponding Layer 2 broadcast domain.
2. VTEP on Switch 1 performs VXLAN message encapsulation based on the obtained egress interface and VNI information, and forwards it to Switch 3.
3. After receiving the VXLAN packet, Switch 3 decapsulates it and finds that the destination MAC in the inner packet is the MAC address of VLAN100, which is the VXLAN Layer 3 gateway interface. Switch 3 then determines that Layer 3 forwarding is needed.
4. Switch 3 strips off the Ethernet encapsulation of the inner packet, obtains the destination IP. Then Switch 3 looks up the routing table according to the destination IP to find the next hop address. Then Switch 3 looks up the ARP table entry according to the next hop address to obtain the destination MAC, VXLAN tunnel egress interface and VNI information.
5. Switch 3 re-encapsulates the VXLAN packet and forwards it to Switch 2, in which the source MAC in the Ethernet header of the inner packet is the MAC address of the VXLAN Layer 3 gateway interface VLAN 200.
6. After receiving the VXLAN packet on Switch 2, VTEP determines the validity of VXLAN packet based on UDP destination port number, source/destination IP address and VNI.

   According to the VNI, the corresponding layer-2 broadcast domain is obtained. Switch 2 then obtains the interface and encapsulation information in the corresponding Layer 2 broadcast domain and performs VXLAN decapsulation on the packet.
7. Switch 2 forwards the message to Server 2 based on the egress interface and encapsulation information.

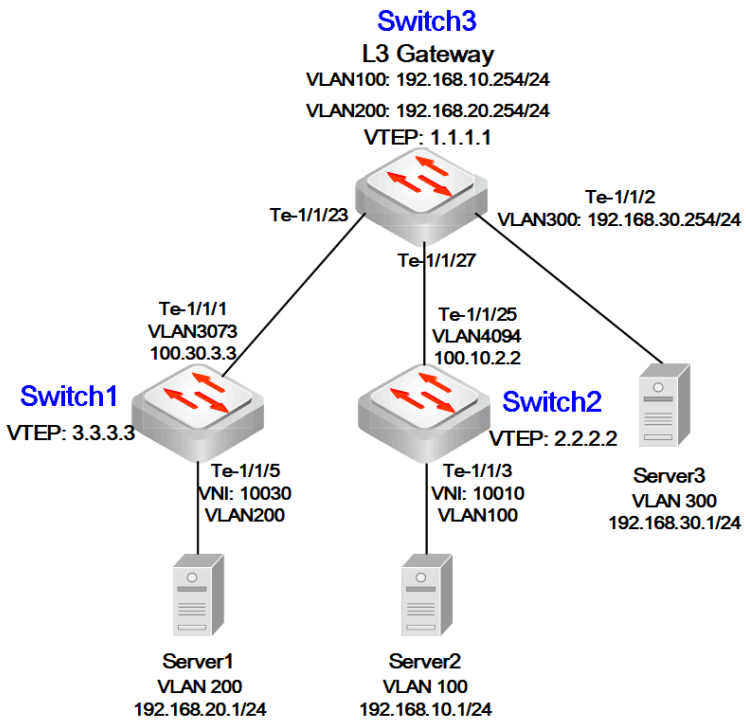
The process of message forwarding from Server 2 to Server 1 is similar and will not be repeated here.

Example for Configuring VXLAN for Different Subnets

- Networking Requirements
  - Figure 1 VXLAN Networking Topology with Centralized Gateway Deployment
- Procedure
  - Switch1
  - Switch2
  - Switch3
- Verify the Configuration

Networking Requirements

Figure 1 VXLAN Networking Topology with Centralized Gateway Deployment



As shown in **Figure 1**, in the centralized gateway scenario, an enterprise has its own servers in different data centers, Server 1 belongs to VLAN 200, Server 2 belongs to VLAN 100 and Server 3 belongs to VLAN 300. Server 1, Server 2 and Server 3 are located in different network segments. Cross-subnet packet forwarding needs to be implemented through a centralized Layer 3 gateway.

Configure different servers on different network segments to communicate with each other through a VXLAN centralized Layer 3 gateway by the following roadmap:

1. Configure static routes on Switch 1, Switch 2, and Switch 3 respectively to ensure network connectivity at the underlay network.
2. Configure VXLAN access network on Switch 1, Switch 2 and Switch 3 respectively to differentiate service flow.
3. Configure VXLAN tunnels on Switch 1, Switch 2 and Switch 3 respectively to forward service flow.
4. To enable users of different network segments to communicate with each other, configure VXLAN Layer 3 gateway on Switch 3. The following steps include how to configure VXLAN Layer 3 gateway:

   a) Configure VXLAN mapping of VNI to VLAN:

   set vxlans vni <*vni_id*> **vlan** <*vlan_id*>

   b) Configure L3 VLAN interface:

   set vlans vlan-id <*vlan_id*> **l3-interface** <*interface_name*>

   c) Configure the IP the L3 VLAN interface:

   set l3-interface vlan-interface <*interface_name*> **address** <*IP_address*> **prefix-length** <*prefix_length*>

Procedure

This section describes the steps of configuring VXLAN for different subnets on Switch1, Switch2 and Switch3.

Switch1

Step 1 Configure the VLANs.

```
admin@Switch1# set vlans vlan-id 200
admin@Switch1# set vlans vlan-id 3073
admin@Switch1# set vlans vlan-id 3073 l3-interface vlan3073
admin@Switch1# set l3-interface vlan-interface vlan3073 address 100.30.3.3 prefix-length 24
admin@Switch1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 3073
admin@Switch1# set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode trunk
admin@Switch1# set interface gigabit-ethernet te-1/1/5 family ethernet-switching vlan members 200
```

Step 2 Enable IP routing and configure the route.

```
admin@Switch1# set ip routing enable true
admin@Switch1# set l3-interface loopback lo address 3.3.3.3 prefix-length 32
admin@Switch1# set protocols static route 1.1.1.1/32 next-hop 100.30.3.4
```

Step 3 Configure VXLAN tunnel.

```
admin@Switch1# set vxlans source-interface lo address 3.3.3.3
admin@Switch1# set vxlans vni 10030 vlan 200
admin@Switch1# set vxlans vni 10030 flood vtep 1.1.1.1
```

Step 4 Commit the configurations.

```
admin@Switch1# commit
```

Switch2

Step 1 Configure the VLANs.

```
admin@Switch2# set vlans vlan-id 100
admin@Switch2# set vlans vlan-id 4094
admin@Switch2# set vlans vlan-id 4094 l3-interface vlan4094
admin@Switch2# set l3-interface vlan-interface vlan4094 address 100.10.2.2 prefix-length 24
admin@Switch2# set interface gigabit-ethernet te-1/1/25 family ethernet-switching native-vlan-id 4094
admin@Switch2# set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode trunk
admin@Switch2# set interface gigabit-ethernet te-1/1/3 family ethernet-switching vlan members 100
```

Step 2 Enable IP routing and configure the route.

```
admin@Switch2# set ip routing enable true
admin@Switch2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@Switch2# set protocols static route 1.1.1.1/32 next-hop 100.10.2.1
```

Step 3 Configure VXLAN tunnel.

```
admin@Switch2# set vxlans source-interface lo address 2.2.2.2
admin@Switch2# set vxlans vni 10010 vlan 100
admin@Switch2# set vxlans vni 10010 flood vtep 1.1.1.1
```

Step 4 Commit the configurations.

```
admin@Switch2# commit
```

Switch3

Step 1 Configure the VLANs.

```
admin@Switch3# set vlans vlan-id 100 l3-interface vlan100
admin@Switch3# set vlans vlan-id 200 l3-interface vlan200
admin@Switch3# set vlans vlan-id 300 l3-interface vlan300
admin@Switch3# set vlans vlan-id 3073 l3-interface vlan3073
admin@Switch3# set vlans vlan-id 4094 l3-interface vlan4094
admin@Switch3# set l3-interface vlan-interface vlan100 address 192.168.10.254 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan200 address 192.168.20.254 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan300 address 192.168.30.254 prefix-length 24
admin@Switch3# set l3-interface vlan-interface vlan3073 address 100.30.3.4 prefix-length 24
```

```
admin@Switch3# set l3-interface vlan-interface vlan4094 address 100.10.2.1 prefix-length 24
admin@Switch3# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 300
admin@Switch3# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@Switch3# set interface gigabit-ethernet te-1/1/23 family ethernet-switching native-vlan-id 3073
admin@Switch3# set interface gigabit-ethernet te-1/1/27 family ethernet-switching native-vlan-id 4094
```

Step 2 Enable IP routing and configure the route.

```
admin@Switch3# set ip routing enable true
admin@Switch3# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@Switch3# set protocols static route 2.2.2.2/32 next-hop 100.10.2.2
admin@Switch3# set protocols static route 3.3.3.3/32 next-hop 100.30.3.3
```

Step 3 Configure VXLAN tunnel.

```
admin@Switch3# set vxlans source-interface lo address 1.1.1.1
admin@Switch3# set vxlans vni 10010 flood vtep 2.2.2.2
admin@Switch3# set vxlans vni 10030 flood vtep 3.3.3.3
```

Step 4 Configure VXLAN mapping of VNI to VLAN.

```
admin@Switch3# set vxlans vni 10010 vlan 100
admin@Switch3# set vxlans vni 10030 vlan 200
```

Step 5 Commit the configurations.

```
admin@Switch3# commit
```

Verify the Configuration

- You can use the **run show vxlan tunnel** command to display the VXLAN tunnel information and tunnel state.

```
admin@Switch1# run show vxlan tunnel
Total number of tunnels: 1

VNI 10030, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:3.3.3.3, dst addr:1.1.1.1, state:UP
  traffic type:all
  nexthops:100.30.3.4
  output ports:te-1/1/1

admin@Switch2# run show vxlan tunnel
Total number of tunnels: 1

VNI 10010, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  nexthops:100.10.2.1
  output ports:te-1/1/25

admin@Switch3# run show vxlan tunnel
Total number of tunnels: 2

VNI 10010, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:1.1.1.1, dst addr:2.2.2.2, state:UP
  traffic type:all
  nexthops:100.10.2.2
  output ports:te-1/1/27

VNI 10030, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:1.1.1.1, dst addr:3.3.3.3, state:UP
  traffic type:all
  nexthops:100.30.3.3
  output ports:te-1/1/23
```

- You can use the **run show vxlan address-table** command to display the VXLAN MAC address table.

```
admin@Switch1# run show vxlan address-table
VNID           MAC address          Type        Interface          VTEP
-----------    -----------------    -------     ----------------   ---------------
10030          00:00:00:00:22:22    Dynamic     te-1/1/5
10030          50:9a:4c:e6:7b:71    Dynamic                        1.1.1.1
Entries in access port:  1
Entries in network port: 1

admin@Switch2# run show vxlan address-table
VNID           MAC address          Type        Interface          VTEP
-----------    -----------------    -------      ---------------  ---------------
10010          00:00:00:00:44:44    Dynamic     te-1/1/3
10010          50:9a:4c:e6:7b:71    Dynamic                        1.1.1.1
Entries in access port:  1
Entries in network port: 1


admin@Switch3# run show vxlan address-table
VNID           MAC address            Type         Interface            VTEP
-----------    -----------------      -------      ----------------     ---------------
10010          00:00:00:00:44:44      Dynamic                           2.2.2.2
10030          00:00:00:00:22:22      Dynamic                           3.3.3.3
Entries in access port:  0
Entries in network port: 2
```

- You can use the **run show vxlan arp** command to display the ARP table on Switch 3.

```
admin@Switch3# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS             VNI         Status     Age          Interface    REMOTE-VTEP
--------------  -----------------     --------      ---------   ----------   -----------   -----------
192.168.10.1     00:00:00:00:44:44     10010       Dynamic      0                          2.2.2.2
192.168.20.1     00:00:00:00:22:22     10030       Dynamic      0                          3.3.3.3
```

VXLAN Configuration Guide

NOTES:

- The switch platforms which use this feature are:
  - Trident2
  - Trident2+
  - Tomahawk
  - Tomahawk+
  - Trident3
  - Maverick
- Tomahawk 2 switches only support VXLAN L2-VNI, not L3-VNI.
- If VXLAN is deployed in an MLAG domain, it behaves a little differently. For details, see MLAG Configuration.

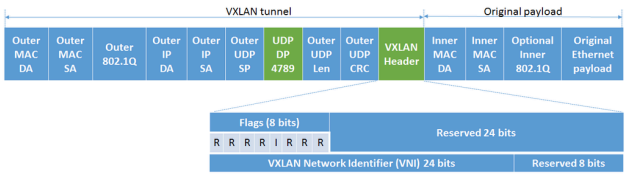
About VXLAN

Virtual Extensible LAN (VXLAN) is an overlay network virtualization technology. An overlay network is a virtual network that is built on top of existing network Layer 2 and Layer 3 technologies to support elastic compute architectures. VXLAN makes it easier for network engineers to scale out a cloud computing environment while logically isolating cloud apps and tenants.

VXLAN Technology

VXLAN uses UDP-based encapsulation to tunnel Ethernet frames and transfers original data packets as tunnel payloads. With the outer UDP tunnel, inner payload data can be quickly transferred on the layer 2 and layer 3 networks. To provide the capability of broadcast domain addressing, the VXLAN technology uses layer 3 IP multicast to replace the Ethernet broadcast. Therefore, the broadcast, unknown unicast, and multicast (BUM) packets can be transferred on virtual networks through broadcasting. For more VXLAN details, please read RFC7348.

VXLAN Packets



As shown in Figure 1-1, a VXLAN packet consists of the outer encapsulation and the inner payloads.

- Flags (8 bits): The flag I must be set to 1 for a valid VXLAN Network Identifier (VNI). The other 7 bits (labeled as R) are reserved fields and must be set to 0 on transmit and ignored on receive.
- VXLAN segment ID or VXLAN VNI: This parameter contains 24 bits and is used to designate the individual VXLAN overlay network on which the VMs are located.
- Reserved fields (24 bits and 8 bits): This parameter must be set to 0 on transmit and ignored on receive.
- The destination port number assigned to the outer tunnel is 4789, which is dedicated.

However, the new addition of VXLAN message encapsulation also introduces a problem with the setting of the MTU value.

In general, the default MTU of a VM or host is 1500 bytes, that is, the maximum original Ethernet message is 1500 bytes.

This message will be encapsulated with a new message header of 50 bytes (VXLAN header 8 bytes + UDP header 8 bytes + external IP h eader 20 bytes + external MAC header 14 bytes) when it is encapsulated with the VXLAN header and goes through the VTEP.
After the encapsulation, the packet size becomes 1550 bytes.
VXLAN packets are not allowed to be fragmented and put back together. It is therefore necessary that all intermediate devices have at least the same MTU if not higher than the originating VXLAN encapsulated packet.

If the original packet of 1500 bytes is encapsulated with VXLAN header, the resulting packet size becomes 1550. If the MTU value of the intermediate device is not convenient to change, then setting the MTU value of the virtual machine to 1450 can also solve this problem temporarily.

VXLAN Inner 802.1Q

Encapsulation mode

Encapsulation means the flow from access ports to network ports. Use one of the following options to specify actions about 802.1Q tag while encapsulation.

- **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged.
- **service-vlan-add**: Add 802.1Q tag for untagged packets, and nothing changed with tagged packets. Encapsulation vlan is required.
- **service-vlan-add-delete**: Add 802.1Q tag for untagged packets, and delete tag for tagged packets. Encapsulation vlan is required.
- **service-vlan-add-replace**: Add 802.1Q tag for untagged packets, and replace tag for tagged packets. Encapsulation vlan is required.
- **service-vlan-delete**: Delete 802.1Q tag for tagged packets, and nothing changed with untagged packets. This is default value according to RFC 7348.
- **service-vlan-replace**: Replace vlan id of 802.1Q tag for tagged packets, and nothing changed with untagged packets. Encapsulation vlan is required.

Decapsulation-mode

Decapsulation means the flow from network ports to access ports.

- **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged.
- **service-vlan-add**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port and vlan, the vlan id of the tag being added will be that vlan, otherwise will be PVID of that port.
- **service-vlan-add-delete**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port and vlan, the vlan id of the tag being added will be that vlan, otherwise will be PVID of that port. From access to access, delete tag for tagged packets.
- **service-vlan-add-replace**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port and vlan, the vlan id of the tag being added will be that vlan, otherwise will be PVID of that port. From access to access, replace tag for tagged packets.This is the default value.
- **service-vlan-delete**: From access to access, delete tag for tagged packets.
- **service-vlan-replace**: From access to access, replace tag for tagged packets.
- **service-vlan-per-port**: The decapsulated packet can be tagged or untagged dynamically based on the setting on the output port.

Based on the above description, please see the following three tables for the detailed traffic changes.

The below table shows the traffic changes in the case that vlans in the access side are binded with a vxlan in the network side.

	Access→Access **(configure with decapsulation mode)**	**Access→Network** **(configure with encapsulation mode)**	**Network→Access** **(configure with decapsulation mode)**
none	untag-->tag(PVID) tag-->remain tag	untag-->tag(PVID) tag->remain tag	untag-->untag tag-->remain tag

service-vlan-add	untag-->tag(PVID) tag->remain tag	untag-->tag(PVID) tag->remain tag	untag-->tag(add vxlan-vlan) tag-->double tag(outer layer add vxlan-vlan)
service-vlan-add-delete	untag-->untag tag-->untag	untag-->untag tag->untag(been deleted)	untag-->tag(add vxlan-vlan) tag-->double tag(outer layer add vxlan-vlan)
service-vlan-add-replace	untag-->tag(PVID) tag-->remain tag	untag→tag(configured VLAN) tag->tag(configured VLAN)	untag-->tag(add vxlan-vlan) tag-->double tag(outer layer add vxlan-vlan)
service-vlan-delete	untag-->untag tag-->untag	untag-->untag tag->untag	untag-->untag tag-->remain tag
service-vlan-replace	untag-->tag(PVID) tag-->remain tag	untag→tag(configured VLAN) tag->tag(changed to encapsulation vlan)	untag-->untag tag-->remain tag
service-vlan-per-port	The decapsulated packet can be tagged or untagged dynamically based on the setting on the output port.		

VXLAN ECMP

In L2/L3, VXLAN ECMP is supported. Picos supports up to 32-way ECMP.

- The VXLAN ECMP does not need special configuration. It entirely depends on the routing ECMP. The route ECMP configure link: ECMP (Equal-Cost Multipath Routing) Configuration
- PicOS uses info from VXLAN header for hash calculation to ensure better performance.

VXLAN Mac Learning

The VTEP performs source MAC learning on the VNI as a Layer 2 switch.

- The switch receives traffic from the local VTEP to the remote VTEP, the VTEP learns the source MAC address in the access port.
- The switch receives traffic from the remote VTEP to the local VTEP, the VTEP learns the source MAC address in the network port.

A VNI MAC address table includes the following types of MAC address entries:

- Access port--Dynamic MAC address entries learned from the local VTEP. VXLAN does not support local configure static MAC address.
- Network port--Include static and dynamic MAC entries.

> **Static mac**--Configure static mac address entries on VXLAN tunnel interfaces.
> **Dynamic mac**--The MAC address entries learned from incoming traffic on VXLAN tunnels. The learned MAC addresses are contained in the inner Ethernet header source MAC.

On network port, the configure static mac entry has higher priority than dynamic mac entries.

VXLAN Traffic Forwarding

Unicast Traffic

- The switch receives traffic from the access port. The VTEP encapsulates the original Ethernet frame with an outer MAC header, outer IP header, and a VXLAN header. The source IP address is the source VTEP's VXLAN tunnel source IP address.
- The local VTEP forwards the encapsulates packets to the VXLAN tunnel a destination IP address.
- The remote VTEP decapsulates the packet and forwards the frame to access port.

Broadcast and Unknown Traffic

- The switch receives traffic from the access port. The VTEP encapsulates the original Ethernet frame with an outer MAC header, outer IP header and a VXLAN header. The source IP address is the source VTEP's VXLAN tunnel source IP address.
- The local VTEP flood encapsulates packets to the VXLAN tunnel all destination IP address.
- The all remote VTEP decapsulates the packet and forwards the frame to access port.

Configure to map VLAN to VXLAN VNI Step

VxLAN supported on PicOS L2/L3 switch. To configure Step, pleae see below.

- Configure VXLAN soure interface

```
set vxlans source-interface loopback address 10.10.10.25
commit
```

- Create VXLAN VNI

```
set vxlans vni 10010
commit
```

- Configure vtep address for VXLAN VNI

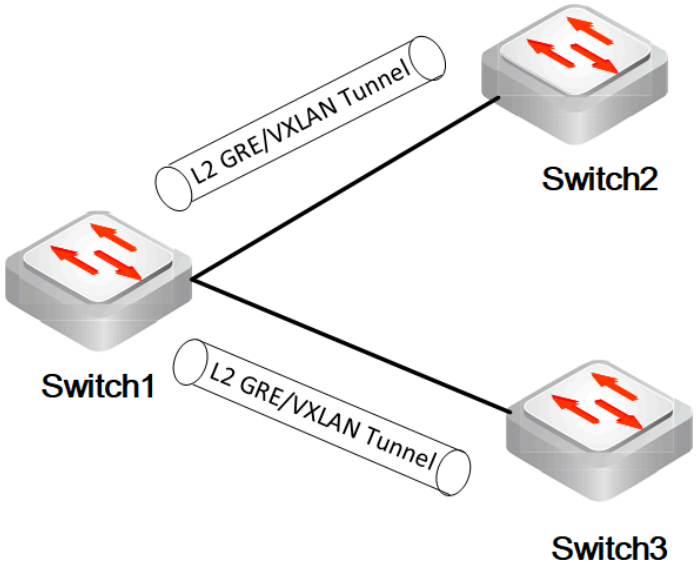
```
set vxlans vni 10010 flood vtep 10.10.10.12
commit
```

- Add vlan into VXLAN VNI

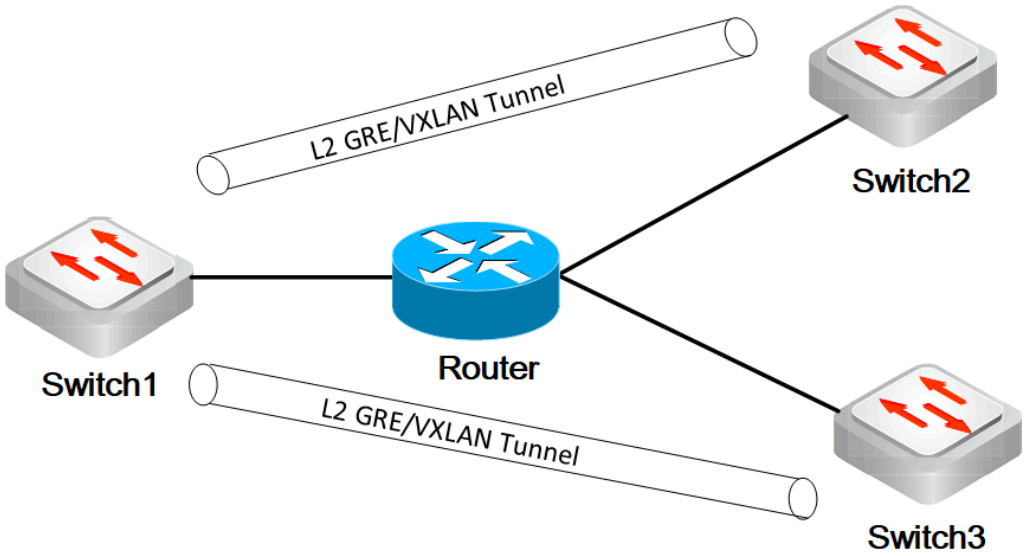
```
set vxlans vni 10010 vlan 100
commit
```

Application Scenario Limitation

In L2 GRE or VXLAN networks, only one next hop is allowed for the same egress interface. In the following figure, the same egress interface on Switch1 has two tunnels, that is, two next hops, which is not allowed.



However, multiple L2 GRE or VXLAN tunnels can exist from the same egress port on Switch1 if connected via the IP router, ensuring that one egress interface has only one next hop, as shown in the figure below.



VXLAN ECMP Configuration

Requirements

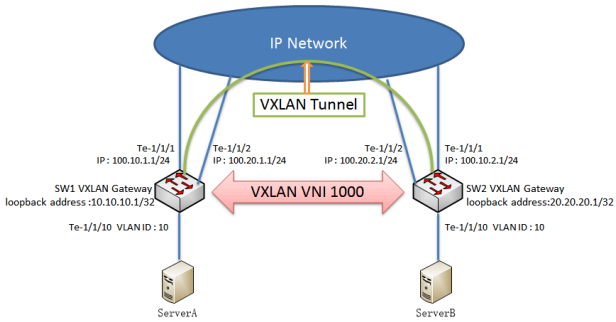
This example uses the following hardware and software components:

- An Trident-II Series switch
- PICOS OS Release more than 2.5 version

Overview

In this example, VXLAN ECMP is configured to run on a VXLAN domain. VTEP interfaces sources are configured to the loopback address. Interfaces are configured for VLAN tagging and encapsulation. Static route protocols is configured to facilitate unicast routing.

Topology



The VXLAN that comprise the networks include:

- SW1 VNI 1000: VTEP 10.10.10.1: VLAN 10
- SW2 VNI 1000: VTEP 20.20.20.1: VLAN 10
- SW1 IP Adress: 100.10.1.1 and IP Address: 100.20.1.1
- SW2 IP Adress: 100.10.2.1 and IP Address: 100.20.2.1

Configuring VXLAN on Trident-II Series Switches

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and copy and paste the commands into the CLI.

SW1 Configure

```
set vlans vlan-id 10
set vlans vlan-id 1000 l3-interface 1000
set vlans vlan-id 2000 l3-interface 2000
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 2000
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
set l3-interface loopback lo address 10.10.10.1 prefix-length 32
set l3-interface vlan-interface 1000 address 100.10.1.1 prefix-length 24
```

```
set l3-interface vlan-interface 2000 address 100.20.1.1 prefix-length 24
set protocols static route 20.20.20.1/32 next-hop 100.10.1.2
set protocols static route 20.20.20.1/32 next-hop 100.20.1.2
set vxlans source-interface lo address 10.10.10.1
set vxlans vni 1000 vlan 10
set vxlans vni 1000 flood vtep 20.20.20.1
commit
```

SW2 Configure

```
set vlans vlan-id 10
set vlans vlan-id 1000 l3-interface 1000
set vlans vlan-id 2000 l3-interface 2000
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 2000
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
set l3-interface loopback lo address 20.20.20.1 prefix-length 32
set l3-interface vlan-interface 1000 address 100.10.2.1 prefix-length 24
set l3-interface vlan-interface 2000 address 100.20.2.1 prefix-length 24
set protocols static route 10.10.10.1/32 next-hop 100.10.2.2
set protocols static route 10.10.10.1/32 next-hop 100.20.2.2
set vxlans source-interface lo address 20.20.20.1
set vxlans vni 1000 vlan 10
set vxlans vni 1000 flood vtep 10.10.10.1
commit
```

Configuring VXLAN Step-by-Step Procedure

The following example shows how to set up a basic VXLAN ECMP configuration with VXLAN domain. To configure VXLAN ECMP on Trident-II Series switches, follow these steps:

Configure VXLAN Step-by-Step for SW1

1. Configure the VLAN ID to 10 for vxlan domain.

```
set vlans vlan-id 10
```

2. Configure the VLAN ID to 1000 and 2000 for ip routing.

```
set vlans vlan-id 1000 l3-interface 1000
set vlans vlan-id 2000 l3-interface 2000
```

3. Configure the te-1/1/1 interface VLAN ID to 1000.

```
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
```

4. Configure the te-1/1/2 interface VLAN ID to 2000.

```
set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 2000
```

5. Configure the te-1/1/10 interface VLAN ID to 10

```
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
```

6. Configure ip address for the loopback interface.

```
set l3-interface loopback lo address 10.10.10.1 prefix-length 32
```

7. Configure ip address and MTU for the vlan-interface 1000.

```
set l3-interface vlan-interface 1000 address 100.10.1.1 prefix-length 24
```

8. Configure ip address and MTU for the vlan-interface 2000.

```
set l3-interface vlan-interface 2000 address 100.20.1.1 prefix-length 24
```

9. Configure static route for the VXLAN ECMP.

```
set protocols static route 20.20.20.1/32 next-hop 100.10.1.2
set protocols static route 20.20.20.1/32 next-hop 100.20.1.2
```

10. Configure VTEP interface sources ip address.

```
set vxlans source-interface lo address 10.10.10.1
```

11. Configure a VLAN ID 10 to a VNI 1000

```
set vxlans vni 1000 vlan 10
```

12. Configure flood vtep ip address for a VNI

```
set vxlans vni 1000 flood vtep 20.20.20.1
```

Configure VXLAN Step-by-Step for SW2

1. Configure the VLAN ID to 10 for vxlan domain.

```
set vlans vlan-id 10
```

2. Configure the VLAN ID to 1000 and 2000 for ip routing.

```
set vlans vlan-id 1000 l3-interface 1000
set vlans vlan-id 2000 l3-interface 2000
```

3. Configure the te-1/1/1 interface VLAN ID to 1000.

```
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 1000
```

4. Configure the te-1/1/2 interface VLAN ID to 2000.

```
set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 2000
```

5. Configure the te-1/1/10 interface VLAN ID to 10

```
set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
```

6. Configure ip address for the loopback interface.

```
set l3-interface loopback lo address 20.20.20.1 prefix-length 32
```

7. Configure ip address and MTU for the vlan-interface 1000.

```
set l3-interface vlan-interface 1000 address 100.10.2.1 prefix-length 24
```

8. Configure ip address and MTU for the vlan-interface 2000.

```
set l3-interface vlan-interface 2000 address 100.20.2.1 prefix-length 24
```

9. Configure static route for the VXLAN ECMP.

```
set protocols static route 10.10.10.1/32 next-hop 100.10.2.2
set protocols static route 10.10.10.1/32 next-hop 100.20.2.2
```

10. Configure VTEP interface sources ip address.

```
set vxlans source-interface lo address 20.20.20.1
```

11. Configure a VLAN ID 10 to a VNI 1000

```
set vxlans vni 1000 vlan 10
```

12. Configure flood vtep ip address for a VNI

```
set vxlans vni 1000 flood vtep 10.10.10.1
```

View the VXLAN tunnel of SW1

Run command **run show vxlan tunnel** to view the information about VXLAN endpoint configuration. Display VXLAN ECMP to the remote vxlan tunnel vtep has two nexthops(100.10.1.2 100.20.1.2).

```
admin@PICOS# run show vxlan tunnel
Total number of tunnels: 1

VNI 1000, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:10.10.10.1, dst addr:20.20.20.1, state:DOWN
  traffic type:all
```

```
  Vtep type:Static
  nexthops:100.10.1.2 100.20.1.2
  output ports:
```

BGP EVPN Configuration Guide

- BGP EVPN Route Types
- Anycast Gateway for EVPN Distributed Networks
- EVPN Symmetric Routing Configuration Example
- EVPN Asymmetric Routing Example
- EVPN With NAC Configuration Guide
- EVPN Multihoming Configuration Guide
- EVPN Enhancements
- Introduction to BGP EVPN

BGP EVPN Route Types

Note
EVPN feature is currently supported on X86 platforms only.

To share routing information with its peers, BGP uses update packets. Routes with the same path attributes are placed in the Network Layer Reachability Information (NLRI) of the update packet and advertised. Since traditional BGP-4 only supports IPv4 unicast routing information, Multiprotocol Extensions for BGP (MP-BGP) was developed to provide additional support for network layer protocols such as multicast and IPv6. MP-BGP extensions are added to the NLRI after which description for different protocols like IPv6 unicast and VPN instance family are subsequently added.

EVPN defines the EVPN sub-address family in the L2VPN address family with the introduction of EVPN NLRI. Once the routes are advertised, VXLAN tunnels are automatically established to carry packets. EVPN NLRI has the following EVPN route types:

- **Type-1, Ethernet Auto-Discovery Routes:** are used for network wide messaging. The Ethernet auto discovery routes are used when a host or server is multihomed to the EVPN VXLAN fabric. It is used to signal to the upstream VTEPs to change their next hop adjacencies for all the MAC addresses associated with a particular ethernet segment in the event of a link failure. The Type-1 EAD routes has the following makeup shown in Table 1. The Ethernet Segment Identifier (ESI) has a non-zero value for multihomed hosts. In case when a device is single-homed, the value of Ethernet Subnet Identifier (ESI) is set to zero. Type-1 routes are advertised on per ESI and per EVI basis and used to achieve fast convergence.

Route Distinguisher (8 Octets)
Ethernet Segment Identifier (10 Octets)
Ethernet Tag ID (4 Octets)
MPLS Label (3 Octets)

Table 1. Ethernet Auto Discovery Route NLRI

- **Type-2, MAC with IP advertisement Routes:** are used to advertise the MAC and IP addresses of hosts. When a VTEP discovers a new host MAC/IP address, it will use Type-2 routes to share this new host with all the other concerned VTEPs in the EVPN VXLAN fabric. This behavior of BGP EVPN is also known as remote host learning and one of the key benefit of having a control plan for VXLAN. The Type-2 route NLRI has the following fields.

Route Distinguisher (8 Octets)
Ethernet Segment Identifier (10 Octets)
Ethernet Tag ID (4 Octets)
MAC Address Length (1 Octet)
MAC Address (6 Octets)
IP Address Length (1 Octet)
IP Address (0, 4 or 16 Octets)
MPLS Label1 (3 Octets)
MPLS Label2 (0 or 3 Octets)

Table 2. EVPN MAC/IP Advertisement Route

- **Type-3, Inclusive Multicast Routes:** are used for the automatic discovery of VTEPs and dynamically establishing VXLAN tunnels. Specifically, Type-3 routes are used to deliver multicast, unknown unicast and broadcast traffic across the EVPN VXLAN fabric. When a VTEP receives a multicast packet encapsulated with a VLAN tag, the ingress VTEP will distribute the packet to all VTEPs that span this VLAN in the given EVPN instance. Type-3 routes have the following NLRI fields.

Route Distinguisher (8 Octets)
Ethernet Tag ID (4 Octets)
IP Address Length (1 Octet)
Originating Router's IP Address (4 or 16 Octets)

Table 3. EVPN Type-3 Route NLRI

- **Type-4, Ethernet Segment Routes:** are needed in multihoming scenarios and used for Designated Forwarder Election. Designated Forwarder is responsible for sending broadcast, unknown unicast and multicast (BUM) traffic to devices on an Ethernet Segment.

  The EVPN NLRI for Type-4 Ethernet Segment Rout consists of the following four fields. For multihomed hosts, the Ethernet Segment Identifier (ESI) must be set to a non-zero value. A value of zero for the ESI indicates a single homed device.

RD (8 Octets)
Ethernet Segment Identifier (10 Octets)
IP Address Length (1 octet)
Originating Router's IP Address (4 or 16 octets)

Table 2. EVPN Type-4 NLRI

- **Type-5, IP Prefix Route:** provides encoding for inter-subnet forwarding. These routes are used for advertising IP prefixes for connectivity between different subnets across the enterprise. Type-5 routes can advertise both IPv4 and IPv6 prefixes. The NLRI fields of IPv4 is shown below.

Route Distinguisher (8 Octets)
Ethernet Segment Identifier (10 Octets)
Ethernet Tag ID (4 Octets)
IP Prefix Length (1 Octet, 0 to 32)
IP Prefix (4 Octets)
Gateway IP Address (4 Octets)
IP Address (0, 4 or 16 Octets)
MPLS Label (3 Octets)

Table 5. Type-5 IPv4 Route NLRI

The NLRI fields in an IPv6 address are given below.

Route Distinguisher (8 Octets)
Ethernet Segment Identifier (10 Octets)
Ethernet Tag ID (4 Octets)
IP Prefix Length (1 Octet, 0 to 128)
IP Prefix (16 Octets)
Gateway IP Address (16 Octets)
IP Address (0, 4 or 16 Octets)
MPLS Label (3 Octets)

Table 6. Type-5 IPv6 Route NLRI

Anycast Gateway for EVPN Distributed Networks

- Introduction
- Configuration Example
- Anycast Gateway over MLAG
  - Configuration Consistency
  - Configuration Notes
  - Example

Introduction

In a data center or campus networks, it is often necessary to implement a seamless migration of virtual machines (VMs) without changing network settings or disrupting the traffic forwarding. Virtual machine migration is just like changing the location of a MAC address in the network. Network infrastructure devices such as switches need to be aware of this change to refresh their forwarding table entries in time to ensure that traffic forwarding is not interrupted.

In EVPN distributed networks, users can configure the same anycast gateway IP and the same virtual MAC (router MAC) on all distributed gateways to enable the anycast gateway function. And also, configure the same IP default gateway address on all hosts or VMS. After that, irrespective of which VTEP the host connected to, as long as they are within the same VNI, they can always use their connected VTEPs as the default gateway to send and receive traffic. Since all hosts within a VLAN are configured with the same IP default gateway address, all hosts or VMs can be easily moved throughout the data center without changing their configuration. This provides flexible VM mobility between different distributed gateways in the network.

You can configure anycast gateway in one of two ways:

- Use the following commands to configure an identical anycast gateway IP address (VLAN interface IP address) and router MAC for anycast gateway.

  set l3-interface vlan-interface <*vlan-interface-name*> **address** <*address*> **prefix-length** <*number*>

  set l3-interface vlan-interface <*vlan-interface-name*> **router-mac** <*macaddr*>

- Use the following commands to configure the anycast gateway IP address (virtual IP address) and anycast gateway MAC (virtual MAC).

  set l3-interface vlan-interface <*interface-name*> **anycast address** <*ip-address*> **prefix-length** <*prefix*>

  set l3-interface vlan-interface <*interface-name*> **anycast mac** <*mac-address*>

NOTEs:

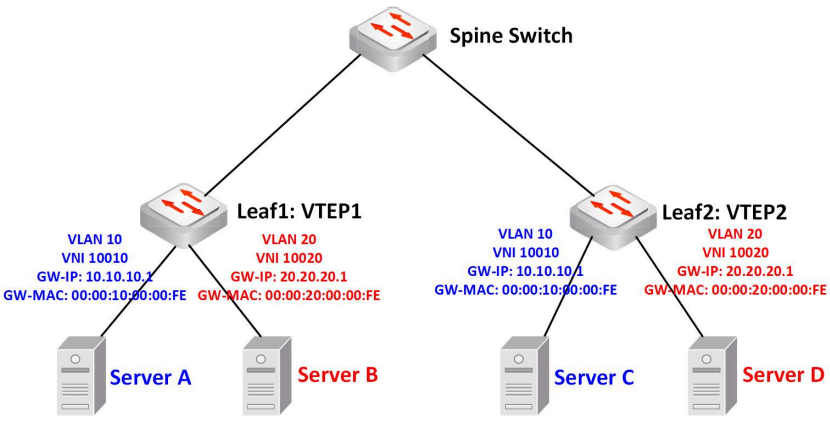
- For anycast gateway over MLAG scenario, only the second way is available.
- When configuring the **Anycast MAC** and **Anycast Address** for an L3 interface, it is necessary to apply both configurations in the same **commit**. This is because these two settings are interdependent, and applying them separately might cause synchronization issues, leading to configuration failures or network instability.

For example,

```
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast address 10.0.1.1 prefix-length 24
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast mac AE:00:10:00:00:FE
admin@Xorplus# commit
```

Configuration Example

For example, as shown in the following simplified EVPN topology, the gateways of the attached servers are on the leaf VTEP switches. Since Server A and Server C are in the same subnet (VLAN: 10/VNI:10010), they should have the same gateway configuration (e.g, gateway IP 10.10.10.1 and gateway MAC 00:00:10:00:00:FE). If Server A moves from Leaf 1 to Leaf 2, the gateway IP configured on Server A doesn't need to be changed. Similarly, Server B and Server D do not need to change their gateway IP and MAC addresses.



When configuring, all VTEPs in the same VNI are required to configure the same anycast gateway IP and virtual MAC.

The example commands below configure anycast gateway on VTEP1 and VTEP2.

```
# Configuring VLAN to VNI mapping
```

```
set vlans vlan-id 10
set vlans vlan-id 20
set vxlans vni 10010 vlan 10
set vxlans vni 10020 vlan 20


# Configuring GW IP
set vlans vlan-id 10 l3-interface vlan10
set vlans vlan-id 20 l3-interface vlan20
set l3-interface vlan-interface vlan10 address 10.10.10.1 prefix-length 24
set l3-interface vlan-interface vlan20 address 20.20.20.1 prefix-length 24


# Configuring GW MAC
set l3-interface vlan-interface vlan10 router-mac 00:00:10:00:00:FE
set l3-interface vlan-interface vlan20 router-mac 00:00:20:00:00:FE
```

NOTEs:

- Anycast gateway can be applied to VTEPs only in the same VLAN/VNI. For example, it is not supported to apply the same anycast gateway within VLAN 10 and VLAN 20 in above case, different gateway configurations for Server A and Server D are required.
- Anycast gateway is mutually exclusive with EVPN **advertise-default-gw** or **advertise-svi-ip** configuration when in the EVPN distributed gateway scenario, they cannot be configured at the same time.

  set protocols bgp [**vrf** <*vrf-name*>] **evpn advertise-default-gw**

  set protocols bgp evpn vni <*vni*> **advertise-svi-ip**

Anycast Gateway over MLAG

Anycast gateway over MLAG function enables VTEP devices to be configured with a single virtual IP address and a single virtual MAC in the form of an anycast IP address and anycast MAC on a pair of MLAG devices. This enables a pair of switches to act as a single VTEP device and seen as such by downstream devices.

In this configuration, two routing devices are combined to form one virtual router, and the virtual IP address is used as the default gateway for hosts to achieve normal communication. When one device in the MLAG pair fails, the other device can still forward traffic normally, thus ensuring reliable network communication.

To ensure proper traffic forwarding, ARP/ND synchronization is performed between the two switches in the MLAG pair every 5 minutes.

MLAG synchronizes ARP/ND entry between the two switches in the MLAG pair; EVPN does not synchronize.

When configuring anycast gateway over MLAG, the following command can be used to configure anycast IP address and anycast MAC address on the MLAG peer devices.

set l3-interface vlan-interface <*interface-name*> **anycast address** <*ip-address*> **prefix-length** <*prefix*>

set l3-interface vlan-interface <*interface-name*> **anycast mac** <*mac-address*>

Besides the anycast IP address and anycast MAC address, IP address of the corresponding access-facing VLAN interface is required to be specified.

set l3-interface vlan-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix*>

NOTE:

For IPv4, the anycast IPv4 address and the VLAN interface IPv4 address should be configured in the same network segment to ensure that the MLAG pair can work normally.

For IPv6, the anycast IPv6 address and the global IPv6 address of the VLAN interface should be configured in the same network segment to ensure that the MLAG pair can work normally.

On the hosts, configure the anycast IP address of the virtual router as the gateway address either statically or through DHCP.

Configuration Consistency

To ensure the pair of MLAG switches continue acting as one single VTEP device, the following configuration needs to be consistent on both devices.

- anycast IP address
- anycast MAC
- VNI on the VXLAN interface (includes both L2 VNI and L3 VNI)
- VTEP address
- RMAC (router MAC), if configured

Configuration Notes

- Anycast gateway over MLAG function and VRRP are mutually exclusive. If anycast gateway over MLAG is configured, VRRP is not allowed to be configured on the same MLAG pair.
- Besides the anycast IP address and anycast MAC address, IP address of the corresponding access-facing VLAN interface is required to be specified through the following command.

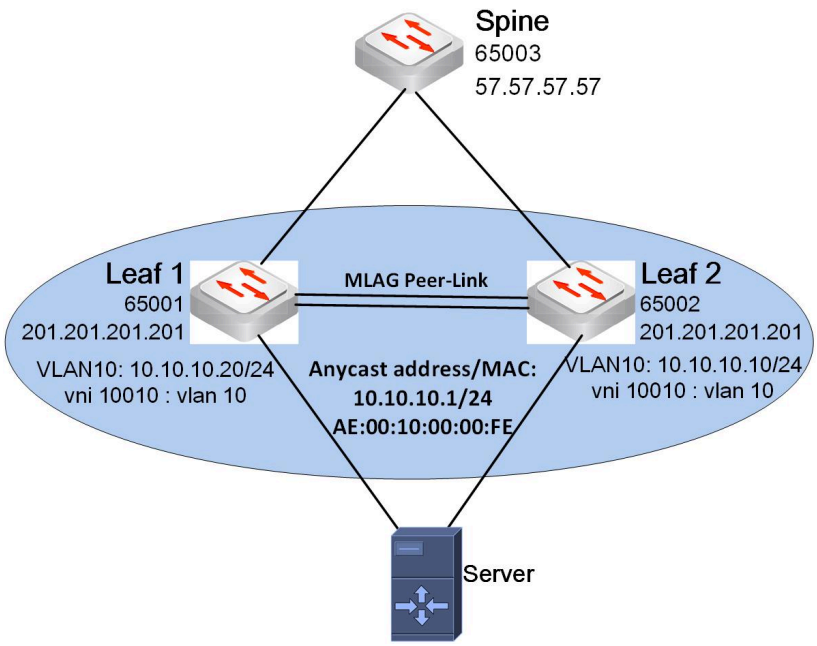
  set l3-interface vlan-interface <*interface-name*> **address** <*ip-address*> **prefix-length** <*prefix*>

- For IPv4, the anycast IPv4 address and the VLAN interface IPv4 address should be configured in the same network segment to ensure that the MLAG pair can work normally.
- For IPv6, the anycast IPv6 address and the global IPv6 address of the VLAN interface should be configured in the same network segment to ensure that the MLAG pair can work normally.
- Anycast IP address list on both devices of MLAG pair must be the same.

Example

As shown in the following simplified EVPN topology, Leaf1 and leaf2 have established VXLAN tunnel with spine. Leaf1 and leaf2 are a pair of MLAG devices.

To enable MLAG pair switches Leaf 1 and Leaf 2 to act as a single virtual router, configure anycast gateway over MLAG on the MLAG pair.



The example commands below can be used to configure anycast gateway over MLAG on Leaf 1 and Leaf 2.

```
# Leaf 1
# Configuring VXLAN source interface.
set l3-interface loopback lo address 201.201.201.201 prefix-length 32
set vxlans source-interface lo address 201.201.201.201

# Configuring VLAN to VNI mapping.
set vlans vlan-id 10
set vxlans vni 10010 vlan 10

# Configuring VXLAN VLAN interface IP address.
set vlans vlan-id 10 l3-interface vlan10
set l3-interface vlan-interface vlan10 address 10.10.10.20 prefix-length 24

# Configuring anycast IP address and anycast MAC.
set l3-interface vlan-interface vlan10 anycast address 10.10.10.1 prefix-length 24
set l3-interface vlan-interface vlan10 anycast mac 00:00:10:00:00:FE


# Leaf 2
# Configuring VXLAN source interface.
set l3-interface loopback lo address 201.201.201.201 prefix-length 32
set vxlans source-interface lo address 201.201.201.201

# Configuring VLAN to VNI mapping.
set vlans vlan-id 10
set vxlans vni 10010 vlan 10

# Configuring VXLAN VLAN interface IP address.
set vlans vlan-id 10 l3-interface vlan10
set l3-interface vlan-interface vlan10 address 10.10.10.10 prefix-length 24

# Configuring anycast IP address and anycast MAC on Leaf 2.
set l3-interface vlan-interface vlan10 anycast address 10.10.10.1 prefix-length 24
set l3-interface vlan-interface vlan10 anycast mac 00:00:10:00:00:FE
```

EVPN Symmetric Routing Configuration Example

- Network Requirments
- Router Configuration
- Verifying Configuration

> **Note**
> EVPN feature is currently supported on X86 platforms only.

Network Requirments

Figure 1 shows our sample topology for EVPN symmetric routing. We have two routers with two servers connected to each router. In this example, Server 1 and Server 2 are in the same network segment, they use L2 VXLAN tunnel for communication. Server 3 and Server 4 are in different network segments, they use L3 VXLAN tunnel for communication. For routed VXLAN traffic within the symmetric IRB model travelling across the same VNI in both directions, same L3 VNI should be configured on Router 1 and Router 2.

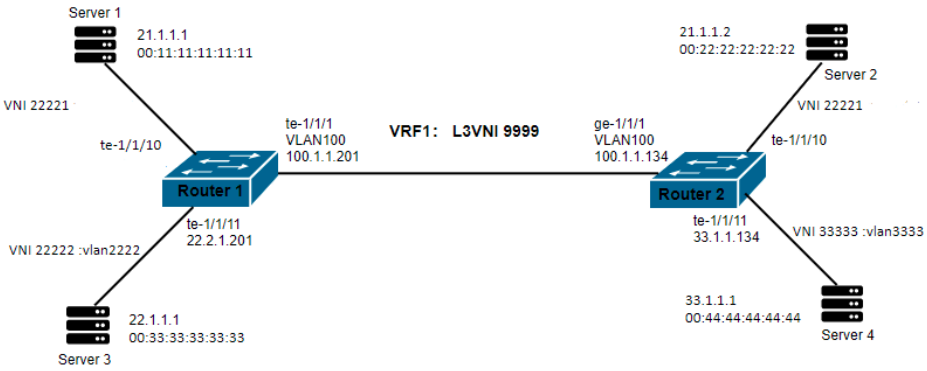


Figure 1. EVPN Symmetric Routing

Router Configuration

The configuration for Router 1 is shown below. The first part of the configuration deals with physical interfaces and assigning VLANs to these interfaces. Router 1 has three physical interfaces configured, two interfaces connecting server 1 and server 3.

Next we setup the layer 3 VLAN interfaces and configure IP addresses for these interfaces.

Then we setup VXLAN VNIs, enable VLAN to VNI mapping and map VNIs to VLAN IDs. Finally we enable IP routing on the device and configure BGP related parameters such as router ID, BGP neighbor and enabling advertising all VNIs.

Follow the detailed configuration steps below.

Router 1 Configuration

Step 1. Configure physical interfaces, VLAN interfaces and assign VLAN IDs and IP addresses.

```
admin@router1# set interface gigabit-ethernet te-1/1/11 family ethernet-switching native-vlan-id 2222
admin@router1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching port-mode trunk
admin@router1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching vlan members 2221
admin@router1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@router1# set l3-interface loopback lo address 201.201.201.201 prefix-length 32
admin@router1# set l3-interface loopback lo address 201.201.201.88 prefix-length 32
admin@router1# set l3-interface vlan-interface vlan100 address 100.1.1.201 prefix-length 24
admin@router1# set l3-interface vlan-interface vlan2222 vrf vrf1
admin@router1# set l3-interface vlan-interface vlan2222 address 22.1.1.201 prefix-length 24
admin@router1# set l3-interface vlan-interface vlan1111 vrf vrf1
admin@router1# set vlans vlan-id 100 l3-interface vlan100
admin@router1# set vlans vlan-id 1111 l3-interface vlan1111
admin@router1# set vlans vlan-id 2221
admin@router1# set vlans vlan-id 2222 l3-interface vlan2222
```

Step 2. Configure VXLAN VNI and map VNI IDs to VLAN IDs. Also create an L3 VNI in vrf1.

> **NOTE:**
> It is recommended to configure the decapsulation mode as "service-vlan-per-port".

```
admin@router1# set vxlans source-interface lo address 201.201.201.201
admin@router1# set vxlans vni 9999 vlan 1111
admin@router1# set vxlans vni 22221 decapsulation mode service-vlan-per-port
admin@router1# set vxlans vni 22221 vlan 2221
admin@router1# set vxlans vni 22222 decapsulation mode service-vlan-per-port
admin@router1# set vxlans vni 22222 vlan 2222
admin@router1# set vxlans vrf vrf1 l3-vni 9999
```

Step 3. Enable IP routing and configure VRF.

```
admin@router1# set ip routing enable true
admin@router1# set ip vrf vrf1
```

Step 4. Configure BGP related configuration.

```
admin@router1# set protocols bgp local-as 201
admin@router1# set protocols bgp ebgp-requires-policy false
admin@router1# set protocols bgp router-id 201.201.201.201
admin@router1# set protocols bgp neighbor 100.1.1.134 remote-as external
admin@router1# set protocols bgp neighbor 100.1.1.134 update-source 100.1.1.201
admin@router1# set protocols bgp neighbor 100.1.1.134 evpn activate true
admin@router1# set protocols bgp ipv4-unicast network 201.201.201.201/32
admin@router1# set protocols bgp ipv4-unicast network 201.201.201.88/32
admin@router1# set protocols bgp evpn advertise-all-vni
admin@router1# set protocols bgp evpn advertise ipv4-unicast
admin@router1# set protocols bgp evpn advertise-svi-ip
admin@router1# set protocols bgp vrf vrf1 local-as 201
admin@router1# set protocols bgp vrf vrf1 router-id 201.201.201.201
admin@router1# set protocols bgp vrf vrf1 ipv4-unicast network 22.1.1.0/24
admin@router1# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
```

Step 5. Commit the configuration.

```
admin@router1# commit
```

Router 2 Configuration

Configuration of Router 2 is shown below. Router 2 also has 3 physical interfaces configured with two interfaces connecting server 2 and server 4. The configuration of Router 2 is almost identical to Router 1 other than the basic configurations like VXLAN VNI and interface IP addresses. The detailed configuration steps are shown below.

Step 1. Configure physical interfaces, VLAN interfaces and assign VLAN ID to physical interfaces and IP addresses.

```
admin@router2# set interface gigabit-ethernet te-1/1/11 family ethernet-switching native-vlan-id 3333
admin@router2# set interface gigabit-ethernet te-1/1/11 family ethernet-switching port-mode trunk
admin@router2# set interface gigabit-ethernet te-1/1/10 family ethernet-switching port-mode trunk
admin@router2# set interface gigabit-ethernet te-1/1/10 family ethernet-switching vlan members 2221
admin@router2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 100
admin@router2# set l3-interface loopback lo address 134.134.134.134 prefix-length 32
admin@router2# set l3-interface vlan-interface vlan100 address 100.1.1.134 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan3333 vrf vrf1
admin@router2# set l3-interface vlan-interface vlan3333 address 33.1.1.134 prefix-length 24
admin@router2# set l3-interface vlan-interface vlan1111 vrf vrf1
admin@router2# set vlans vlan-id 100 l3-interface vlan100
admin@router2# set vlans vlan-id 1111 l3-interface vlan1111
admin@router2# set vlans vlan-id 2221
admin@router2# set vlans vlan-id 3333 l3-interface vlan3333
```

Step 2: Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
admin@router2# set vxlans source-interface lo address 134.134.134.134
admin@router2# set vxlans vni 9999 vlan 1111
admin@router2# set vxlans vni 22221 decapsulation mode service-vlan-per-port
admin@router2# set vxlans vni 22221 vlan 2221
admin@router2# set vxlans vni 33333 vlan 3333
admin@router2# set vxlans vni 3333 decapsulation mode service-vlan-per-port
admin@router2# set vxlans vrf vrf1 l3-vni 9999
```

Step 3: Enable IP routing and configure VRF.

```
admin@router2# set ip routing enable true
admin@router2# set ip vrf vrf1
```

Step 4: Configure BGP related configuration

```
admin@router2# set protocols bgp local-as 134
admin@router2# set protocols bgp ebgp-requires-policy false
admin@router2# set protocols bgp router-id 134.134.134.134
admin@router2# set protocols bgp neighbor 100.1.1.201 remote-as external
admin@router2# set protocols bgp neighbor 100.1.1.201 update-source 100.1.1.134
admin@router2# set protocols bgp neighbor 100.1.1.201 evpn activate true
admin@router2# set protocols bgp ipv4-unicast network 134.134.134.134/32
admin@router2# set protocols bgp evpn advertise-all-vni
admin@router2# set protocols bgp evpn advertise-svi-ip
admin@router2# set protocols bgp vrf vrf1 local-as 134
admin@router2# set protocols bgp vrf vrf1 router-id 134.134.134.134
admin@router2# set protocols bgp vrf vrf1 ipv4-unicast network 33.1.1.0/24
admin@router2# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
```

Step 5. Commit the configuration.

```
admin@router2# commit
```

Verifying Configuration

- To check the BGP state and neighbor status on Router 2, we will run the **run show bgp neighbor** command.

```
admin@router2# run show bgp neighbor 100.1.1.201
BGP neighbor is 100.1.1.201, remote AS 201, local AS 134, external link
Hostname: 51.201
 Member of peer-group fabric for session parameters
  BGP version 4, remote router ID 201.201.201.201, local router ID 134.134.134.134
  BGP state = Established, up for 01:22:43
```

- To check the BGP EVPN MAC address table, we will run the command **run show vxlan address-table** as shown below.

```
admin@router1# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------   ---------------
9999           18:5a:58:37:64:61    Dynamic                       134.134.134.134
22221          00:11:11:11:11:11    Dynamic    te-1/1/10
22221          00:22:22:22:22:22    Dynamic                       134.134.134.134
22222          00:33:33:33:33:33    Dynamic    te-1/1/11
Entries in access port:  2
Entries in network port: 2


admin@router2# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------   ---------------
9999           18:5a:58:37:55:e1    Dynamic                       201.201.201.201
22221          00:11:11:11:11:11    Dynamic                       201.201.201.201
22221          00:22:22:22:22:22    Dynamic    te-1/1/10
33333          00:44:44:44:44:44    Dynamic    te-1/1/11
Entries in access port:  2
Entries in network port: 2
```

- To verify the VXLAN tunnel information, run the command **run show vxlan tunnel**.

```
admin@router1# run show vxlan tunnel
Total number of tunnels: 2

VNI 9999, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:201.201.201.201, dst addr:134.134.134.134, state:UP
  traffic type:unicast
  Vtep type:EVPN
```

```
  nexthops:100.1.1.134
  output ports:te-1/1/1

VNI 22221, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:201.201.201.201, dst addr:134.134.134.134, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:100.1.1.134
  output ports:te-1/1/1



admin@router2# run show vxlan tunnel
Total number of tunnels: 2

VNI 9999, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:134.134.134.134, dst addr:201.201.201.201, state:UP
  traffic type:unicast
  Vtep type:EVPN
  nexthops:100.1.1.201
  output ports:ge-1/1/1

VNI 22221, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:134.134.134.134, dst addr:201.201.201.201, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:100.1.1.201
  output ports:ge-1/1/1
```

- Run the command **run show vxlan evpn rmac** to display the Router-MAC (rmac) and other VXLAN parameters. Note that to configure rmac for a layer 3 VLAN interface, run the command **set l3-interface vlan-interface** <*interface-name*> **router-mac** <*router-mac*>. The system MAC of the switch is displayed if the router MAC is not configured.

```
admin@router1# run show vxlan evpn rmac
L3-VNI    Interface      SVI-Interface  Remote-VTEP      Neighbor-RMAC      Flags
--------  -------------  -------------  ---------------  -----------------  -----
9999      vxlan9999      vlan1111       134.134.134.134  18:5a:58:37:64:61  0x16



admin@router2# run show vxlan evpn rmac
L3-VNI    Interface      SVI-Interface  Remote-VTEP      Neighbor-RMAC      Flags
--------  -------------  -------------  ---------------  -----------------  -----
9999      vxlan9999      vlan1111       201.201.201.201  18:5a:58:37:55:e1  0x16
```

- To display the VXLAN EVPN routes, run the command **run show vxlan evpn route.**

```
admin@router1# run show vxlan evpn route ipv4
VRF       ROUTE              NextHop          VNI         Interface
--------  -----------------  ---------------  ----------  -----------------
vrf1      33.1.1.1/32        134.134.134.134  9999        vlan1111
vrf1      33.1.1.134/32      134.134.134.134  9999        vlan1111
vrf1      33.1.1.0/24        134.134.134.134  9999        vlan1111



admin@router2# run show vxlan evpn route ipv4
VRF       ROUTE              NextHop          VNI         Interface
--------  -----------------  ---------------  ----------  -----------------
vrf1      22.1.1.1/32        201.201.201.201  9999        vlan1111
vrf1      22.1.1.201/32      201.201.201.201  9999        vlan1111
vrf1      22.1.1.0/24        201.201.201.201  9999        vlan1111
```

- To check the ARP table of a device, run the command **run show vxlan arp.**

```
admin@router1# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS        VNI        Status     Age       Interface      REMOTE-VTEP
---------------  -----------------  --------  ---------   -------   ----------    ------------
22.1.1.1         00:33:33:33:33:33  22222     Dynamic     23         te-1/1/11
```

```
admin@router2# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS        VNI       Status     Age    Interface     REMOTE-VTEP
---------------  -----------------  --------  --------  ------  ----------    ------------
33.1.1.1         00:44:44:44:44:44  33333     Dynamic   26      te-1/1/11
```

EVPN Asymmetric Routing Example

- Network Requirements
- Router Configuration
- Verify Configuration

> **Note**
> EVPN feature is only available on X86 platforms.

Network Requirements

PICOS version 4.0 and higher offer both Symmetric and Asymmetric routing for BGP EVPN hosts. In this document we will examine the case of Asymmetric EVPN routing with two hosts in different VNIs on two devices, R1 and R2.

Figure 1 depicts how packet exchange between two hosts occurs in asymmetric BGP EVPN routing model. In the asymmetric routing model, the two end hosts, Host1 and Host2 are in two different VLANs and different VNIs. Host1 intends to communicate with Host2, sends a packet with destination MAC address of of R1 because R1 is configured as the gateway on Host1. On R1, the gateway is configured on an interface that belongs to VNI 30. The packet from Host1 on ingress at R1 is first routed to VNI 30 within R1 and then bridged to R2 over the VXLAN tunnel VNI 30. On receiving the packet, R2 will strip off the VXLAN header and forward the packet to Host2.

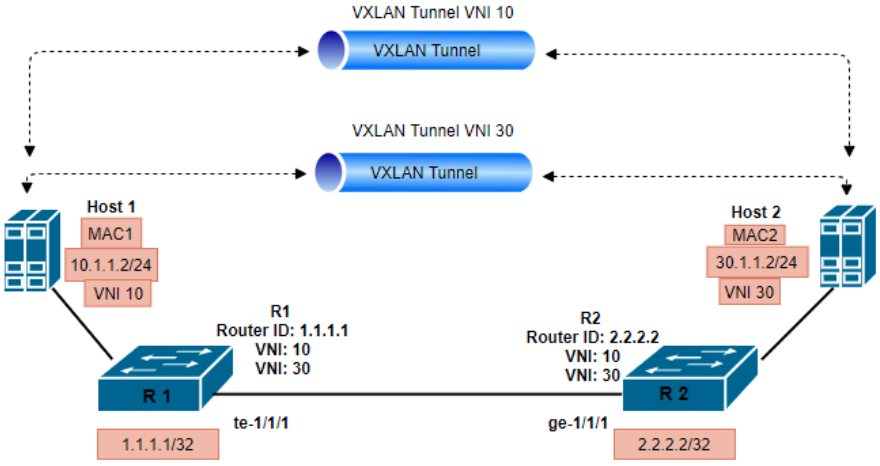


Figure 1. EVPN Asymmetric Routing Model

The one limitation in this model is that both the devices must have the two VXLAN VNIs configured regardless if there are any hosts connected to it. In Figure 1, Host1 belongs to VNI 10 but both VNI 10 and VNI 30 are configured on R1. Similarly, Host2 belongs to VNI 30 but both VNI 10 and VNI 30 are configured on R2 for asymmetric routing to work properly.

Router Configuration

R1 Configuration

Step 1 Configure VLAN ID, L3 VLAN interfaces loopback interfaces and IP addressing. Interface te-1/1/15 connects to Host1.

NOTE: "router-mac" is an optional configuration for anycast gateway.

```
admin@R1# set vlans vlan-id 10 l3-interface vlan10
admin@R1# set vlans vlan-id 30 l3-interface vlan30
admin@R1# set vlans vlan-id 1111 l3-interface vlan1111
admin@R1# set vlans vlan-id 4094 l3-interface vlan4094
admin@R1# set interface gigabit-ethernet te-1/1/15 family ethernet-switching native-vlan-id 10
admin@R1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 4094
admin@R1# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@R1# set l3-interface loopback vrf1 address 201.201.201.201 prefix-length 32
admin@R1# set l3-interface vlan-interface vlan4094 address 40.94.0.2 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan1111 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan10 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan10 router-mac 00:00:10:00:00:FE
admin@R1# set l3-interface vlan-interface vlan10 address 10.1.1.10 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan30 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan30 router-mac 00:00:30:00:00:FE
```

```
admin@R1# set l3-interface vlan-interface vlan30 address 30.1.1.30 prefix-length 24
```

Step 2 Configure VXLAN VNI and map VNI IDs to VLAN IDs.

> **NOTEs:**
> - When anycast gateway is configured, it is recommended to configure ARP/ND suppression at the same time.
> - It is recommended to configure the decapsulation mode as "service-vlan-per-port".

```
admin@R1# set vxlans source-interface lo address 1.1.1.1
admin@R1# set vxlans vni 100 vlan 1111
admin@R1# set vxlans vni 10 decapsulation mode service-vlan-per-port
admin@R1# set vxlans vni 10 vlan 10
admin@R1# set vxlans vni 10 arp-nd-suppress disable false
admin@R1# set vxlans vni 30 decapsulation mode service-vlan-per-port
admin@R1# set vxlans vni 30 vlan 30
admin@R1# set vxlans vni 30 arp-nd-suppress disable false
admin@R1# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
```

Step 3 Enable IP routing and configure VRF and hostname.

```
admin@R1# set system hostname R1
admin@R1# set ip routing enable true
admin@R1# set ip vrf vrf1
```

Step 4 Configure BGP and OSPF related configuration.

> **NOTE:**
> The **set protocols bgp evpn advertise ipv4-unicast** command is used to announce IPv4 prefixes in the BGP RIB as EVPN Type-5 routes. To announce IPv6 prefixes in the BGP RIB as EVPN Type-5 routes, use command **set protocols bgp evpn advertise ipv6-unicast**.

```
admin@R1# set protocols bgp local-as 65001
admin@R1# set protocols bgp router-id 1.1.1.1
admin@R1# set protocols bgp neighbor 2.2.2.2 remote-as internal
admin@R1# set protocols bgp neighbor 2.2.2.2 update-source 1.1.1.1
admin@R1# set protocols bgp neighbor 2.2.2.2 evpn activate true
admin@R1# set protocols bgp ipv4-unicast
admin@R1# set protocols bgp evpn advertise-all-vni
admin@R1# set protocols bgp evpn advertise ipv4-unicast
admin@R1# set protocols bgp evpn advertise-svi-ip
admin@R1# set protocols bgp vrf vrf1 local-as 65001
admin@R1# set protocols bgp vrf vrf1 router-id 1.1.1.1
admin@R1# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@R1# set protocols ospf router-id 1.1.1.1
admin@R1# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
admin@R1# set protocols ospf network 1.1.1.1/32 area 0.0.0.0
admin@R1# set vlans vlan-id 10 l3-interface vlan10
admin@R1# set vlans vlan-id 30 l3-interface vlan30
admin@R1# set vlans vlan-id 1111 l3-interface vlan1111
admin@R1# set vlans vlan-id 4094 l3-interface vlan4094
```

Step 5 Commit the configuration.

```
admin@R1# commit
```

R2 Configuration

Step 1 Configure VLAN ID, L3 VLAN interfaces loopback interfaces and IP addresses. Interface ge-1/1/15 connects to Host2.

```
admin@R2# set vlans vlan-id 10 l3-interface vlan10
admin@R2# set vlans vlan-id 30 l3-interface vlan30
admin@R2# set vlans vlan-id 1111 l3-interface vlan1111
admin@R2# set vlans vlan-id 4094 l3-interface vlan4094
admin@R2# set interface gigabit-ethernet ge-1/1/15 family ethernet-switching native-vlan-id 30
admin@R2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 4094
admin@R2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
admin@R2# set l3-interface loopback vrf1 address 134.134.134.134 prefix-length 32
admin@R2# set l3-interface vlan-interface vlan1111 vrf vrf1
```

```
admin@R2# set l3-interface vlan-interface vlan4094 address 40.94.0.1 prefix-length 24
admin@R2# set l3-interface vlan-interface vlan10 vrf vrf1
admin@R2# set l3-interface vlan-interface vlan10 router-mac 00:00:10:00:00:FE
admin@R2# set l3-interface vlan-interface vlan10 address 10.1.1.10 prefix-length 24
admin@R2# set l3-interface vlan-interface vlan30 vrf vrf1
admin@R2# set l3-interface vlan-interface vlan30 router-mac 00:00:30:00:00:FE
admin@R2# set l3-interface vlan-interface vlan30 address 30.1.1.30 prefix-length 24
```

Step 2 Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
admin@R2# set vxlans source-interface lo address 2.2.2.2
admin@R2# set vxlans vni 100 vlan 1111
admin@R2# set vxlans vni 10 decapsulation mode service-vlan-per-port
admin@R2# set vxlans vni 10 vlan 10
admin@R2# set vxlans vni 10 arp-nd-suppress disable false
admin@R2# set vxlans vni 30 decapsulation mode service-vlan-per-port
admin@R2# set vxlans vni 30 vlan 30
admin@R2# set vxlans vni 30 arp-nd-suppress disable false
admin@R2# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
```

Step 3 Enable IP routing and configure VRF and hostname.

```
admin@R2# set system hostname R2
admin@R2# set ip routing enable true
admin@R2# set ip vrf vrf1
```

Step 4 Configure BGP and OSPF related configuration

```
admin@R2# set protocols bgp local-as 65001
admin@R2# set protocols bgp router-id 2.2.2.2
admin@R2# set protocols bgp neighbor 1.1.1.1 remote-as internal
admin@R2# set protocols bgp neighbor 1.1.1.1 update-source 2.2.2.2
admin@R2# set protocols bgp neighbor 1.1.1.1 evpn activate true
admin@R2# set protocols bgp evpn advertise-all-vni
admin@R2# set protocols bgp evpn advertise ipv4-unicast
admin@R2# set protocols bgp evpn advertise-svi-ip
admin@R2# set protocols bgp vrf vrf1 local-as 65001
admin@R2# set protocols bgp vrf vrf1 router-id 2.2.2.2
admin@R2# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@R2# set protocols lldp enable true
admin@R2# set protocols spanning-tree enable false
admin@R2# set protocols ospf router-id 2.2.2.2
admin@R2# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
admin@R2# set protocols ospf network 2.2.2.2/32 area 0.0.0.0
```

Step 5 Commit the configuration.

```
admin@R2# commit
```

Verify Configuration

- On R1 and R2, run the command **run show route vrf vrf1 forward-host ipv4 all** to display the host routes.

```
admin@R1# run show route vrf vrf1 forward-host ipv4 all
Address           HWaddress           Port
---------------   -----------------   ---------
10.1.1.2         00:1E:C9:BB:C0:3C   vxlan-0x80000002
30.1.1.2         00:0C:29:77:8B:15   vxlan-0x80000001
Total host count:2


admin@R2# run show route vrf vrf1 forward-host ipv4 all
Address           HWaddress           Port
---------------   -----------------   ---------
10.1.1.2          00:1E:C9:BB:C0:3C   vxlan-0x80000001
30.1.1.2          00:0C:29:77:8B:15   vxlan-0x80000003
```

```
Total host count:2
```

- Run the command **run show vxlan arp** on either R1 or R2 to check VXLAN ARP table.

```
admin@R1# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS        VNI        Status     Age        Interface      REMOTE-VTEP
---------------  -----------------  ---------  --------   ----------  ------------    ----------
10.1.1.2        00:1e:c9:bb:c0:3c  10          Dynamic    135         te-1/1/15
30.1.1.2        00:0c:29:77:8b:15  30          Static                                 2.2.2.2


admin@R2# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS         VNI        Status    Age         Interface      REMOTE-VTEP
---------------  -----------------  ---------  ---------  ----------   ---------      ----------
10.1.1.2         00:1e:c9:bb:c0:3c   10         Static                                 1.1.1.1
30.1.1.2         00:0c:29:77:8b:15   30         Dynamic  168          ge-1/1/15
```

- Run the command **run show vxlan address-table** to display the VXLAN address table.

```
admin@R1# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------   ---------------
10             00:1e:c9:bb:c0:3c    Dynamic    te-1/1/15
30             00:0c:29:77:8b:15    Dynamic                       2.2.2.2
30             00:50:56:65:5c:b2    Dynamic                       2.2.2.2
Entries in access port:  1
Entries in network port: 2



admin@R2# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------   ---------------
10             00:1e:c9:bb:c0:3c    Dynamic                       1.1.1.1
30             00:0c:29:77:8b:15    Dynamic    ge-1/1/15
30             00:50:56:65:5c:b2    Dynamic    ge-1/1/15
Entries in access port:  2
Entries in network port: 1
```

- To check the VXLAN tunnels on either devices, run the command **run show vxlan tunnel.**

```
admin@R1# run show vxlan tunnel
Total number of tunnels: 2

VNI 10, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:1.1.1.1, dst addr:2.2.2.2, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.1
  output ports:te-1/1/1

VNI 30, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:1.1.1.1, dst addr:2.2.2.2, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.1
  output ports:te-1/1/1



admin@R2# run show vxlan tunnel
Total number of tunnels: 2

VNI 10, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1
```

```
VNI 30, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1
```

EVPN With NAC Configuration Guide

In this configuration example we will examine the EVPN with NAC use case. As shown in Figure 1 below, we have two Pica8 switches in this topology. Switch R1 has a Cisco IP phone connected with it. Switch1 is also connected with our management network that gives it access to Cisco ISE network access controller. Similarly switch R2 is also connected with a host and an IP phone.

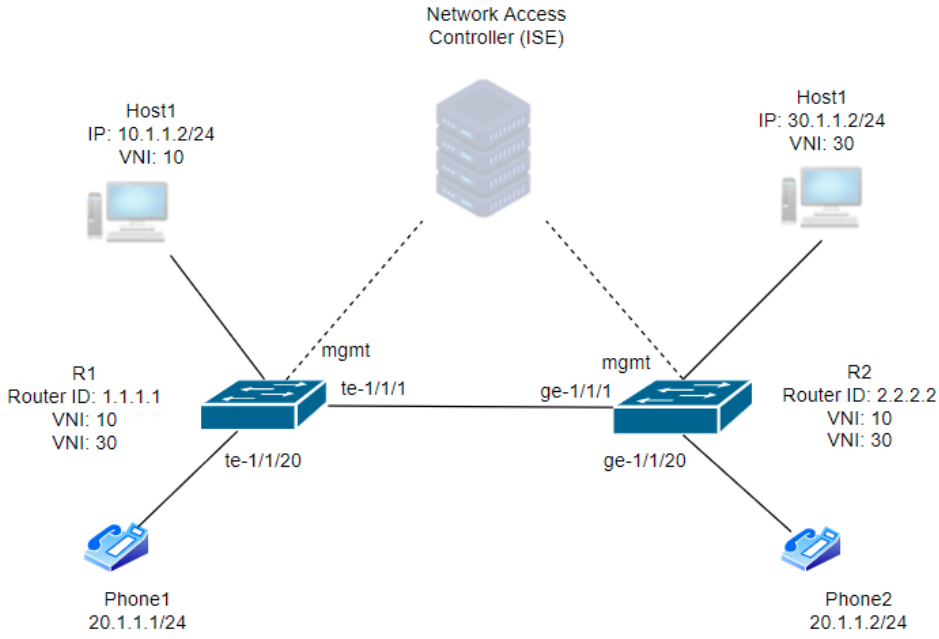


Figure 1. EVPN with NAC Topology

The general idea in this use case is that we will first program ISE to recognize any MAB authentication requests for this IP phone device and assign it a dynamic VLAN through the Access-Accept message. This will cause the switch to put the physical port connecting the IP phone into a VLAN which is part of the VXLAN network through VLAN to VNI mapping. Once part of that VNI, the IP phone can then be accessible throughout the VXLAN network. The communication between the IP phone and other devices will pass through the VXLAN tunnel if the devices are physically located on different switches. The phone can then be managed by some kind of phone management or call manager software to establish phone connectivity throughout the network however, such configuration details are beyond the scope of this document.

The routing model used in this topology for the host computers is the EVPN Asymmetric routing model in which, when two communicating devices reside in two different VNIs, routing will take place locally on the device from one VNI to the target VNI and then data packets are bridged from one switch to the other switch and forwarded to the destination device. Since ISE will usually profile IP phone devices and put them all into a single VLAN or voice VLAN, hence such devices will belong to the same VNI even if they are connected to different switches. In this example topology, ISE will assign the dynamic VLAN ID 20 to both the IP phone devices.

Switch Configuration

This section details the configuration of the two switch devices in this topology.

R1 Switch Configuration

Step 1: Configure VLAN ID, L3 VLAN interfaces loopback interfaces and IP addressing. Interface te-1/1/10 connects to PC1 and interface te-1/1/20 connects to the IP phone.

```
admin@R1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 4094
admin@R1# set interface gigabit-ethernet te-1/1/20 family ethernet-switching port-mode trunk
admin@R1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 10
admin@R1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
admin@R1# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@R1# set l3-interface loopback vrf1 address 201.201.201.201 prefix-length 32
admin@R1# set l3-interface vlan-interface vlan4094 address 40.94.0.2 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan10 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan20 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan30 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan10 address 10.1.1.201 prefix-length 24
```

```
admin@R1# set l3-interface vlan-interface vlan20 address 20.1.1.201 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan1111 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan1111 router-mac 00:16:16:16:16:16
admin@R1# set vlans vlan-id 20 l3-interface vlan20
admin@R1# set vlans vlan-id 10 l3-interface vlan10
admin@R1# set vlans vlan-id 30 l3-interface vlan30
admin@R1# set vlans vlan-id 1111 l3-interface vlan1111
admin@R1# set vlans vlan-id 4094 l3-interface vlan4094
```

Step 2: Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
admin@R1# set vxlans source-interface lo address 1.1.1.1
admin@R1# set vxlans vni 100 vlan 1111
admin@R1# set vxlans vni 10 vlan 10
admin@R1# set vxlans vni 30 vlan 30
admin@R1# set vxlans vni 20 vlan 20
admin@R1# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
admin@R1# set vxlans source-interface lo address 1.1.1.1
```

Step 3: Enable IP routing and configure VRF and hostname.

```
admin@R1# set ip routing enable true
admin@R1# set ip vrf vrf1
```

Step 4: Configure BGP and OSPF related configuration

```
admin@R1# set protocols bgp local-as 65001
admin@R1# set protocols bgp router-id 1.1.1.1
admin@R1# set protocols bgp neighbor 2.2.2.2 remote-as internal
admin@R1# set protocols bgp neighbor 2.2.2.2 update-source 1.1.1.1
admin@R1# set protocols bgp neighbor 2.2.2.2 evpn activate true
admin@R1# set protocols bgp ipv4-unicast
admin@R1# set protocols bgp evpn advertise-all-vni
admin@R1# set protocols bgp evpn advertise ipv4-unicast
admin@R1# set protocols bgp vrf vrf1 local-as 65001
admin@R1# set protocols bgp vrf vrf1 router-id 1.1.1.1
admin@R1# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@R1# set protocols ospf router-id 1.1.1.1
admin@R1# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
admin@R1# set protocols ospf network 1.1.1.1/32 area 0.0.0.0
```

Step 5: Configure 802.1X and NAC. Specify the NAS IP, the authentication server IP which is the IP address of the ISE server in this case and authentication mode.

```
admin@R1# set protocols dot1x interface te-1/1/20 host-mode multiple
admin@R1# set protocols dot1x interface te-1/1/20 auth-mode mac-radius
admin@R1# set protocols dot1x aaa radius authentication server-ip 10.10.50.65 shared-key test
admin@R1# set protocols dot1x aaa radius nas-ip 10.10.51.201
```

Step 6: Enable POE for interface te-1/1/20. We need this step to power up the phone device using the switch's' POE feature without needing an external power source.

```
admin@R1# set poe interface te-1/1/20
```

R2 Configuration

Step 1: Configure VLAN ID, L3 VLAN interfaces, loopback interfaces and IP addresses. Interface ge-1/1/10 connects to PC2 and interface ge-1/1/20 connects to the IP phone.

```
root@R2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 4094
root@R2# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching native-vlan-id 30
root@R2# set interface gigabit-ethernet ge-1/1/20 family ethernet-switching port-mode trunk
root@R2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
root@R2# set l3-interface loopback vrf1 address 134.134.134.134 prefix-length 32
```

```
root@R2# set l3-interface vlan-interface vlan1111 vrf vrf1
root@R2# set l3-interface vlan-interface vlan30 vrf vrf1
root@R2# set l3-interface vlan-interface vlan20 vrf vrf1
root@R2# set l3-interface vlan-interface vlan30 address 30.1.1.134 prefix-length 24
root@R2# set l3-interface vlan-interface vlan20 address 20.1.1.134 prefix-length 24
root@R2# set l3-interface vlan-interface vlan4094 address 40.94.0.1 prefix-length 24
root@R2# set vlans vlan-id 10 l3-interface vlan10
root@R2# set vlans vlan-id 20 l3-interface vlan20
root@R2# set vlans vlan-id 30 l3-interface vlan30
```

Step 2: Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
root@R2# set vlans vlan-id 1111 l3-interface vlan1111
root@R2# set vlans vlan-id 4094 l3-interface vlan4094
root@R2# set vxlans source-interface lo address 2.2.2.2
root@R2# set vxlans vni 100 vlan 1111
root@R2# set vxlans vni 10 vlan 10
root@R2# set vxlans vni 20 vlan 20
root@R2# set vxlans vni 30 vlan 30
```

Step 3: Enable IP routing and configure VRF and hostname.

```
root@R2# set system hostname R2
root@R2# set ip routing enable true
root@R2# set ip vrf vrf1
```

Step 4: Configure BGP and OSPF related configuration

```
root@R2# set protocols bgp local-as 65001
root@R2# set protocols bgp router-id 2.2.2.2
root@R2# set protocols bgp neighbor 1.1.1.1 remote-as internal
root@R2# set protocols bgp neighbor 1.1.1.1 update-source 2.2.2.2
root@R2# set protocols bgp neighbor 1.1.1.1 evpn activate true
root@R2# set protocols bgp evpn advertise-all-vni
root@R2# set protocols bgp evpn advertise ipv4-unicast
root@R2# set protocols bgp vrf vrf1 local-as 65001
root@R2# set protocols bgp vrf vrf1 router-id 2.2.2.2
root@R2# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
root@R2# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
root@R2# set protocols ospf router-id 2.2.2.2
root@R2# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
root@R2# set protocols ospf network 2.2.2.2/32 area 0.0.0.0
```

Step 5: Configure 802.1X and NAC. Specify the NAS IP, the authentication server IP which is the IP address of the ISE server in this case and the authentication mode.

```
admin@R2# set protocols dot1x interface ge-1/1/20 host-mode multiple
admin@R2# set protocols dot1x interface ge-1/1/20 auth-mode mac-radius
admin@R2# set protocols dot1x aaa radius authentication server-ip 10.10.50.65 shared-key test
admin@R2# set protocols dot1x aaa radius nas-ip 10.10.51.134
```

Step 6: Enable POE for interface ge-1/1/20. We need this step to power up the phone device using the switch's' POE feature.

```
admin@R2# set poe interface ge-1/1/20
```

Note: In a more realistic network environment, DHCP access needs to be allowed in the VLAN connecting the IP phone devices to automatically assign IP address and other basic network information like DNS and gateway details. Such configurations are not implemented in this example topology.

Verify Configuration

After successful authentication from the ISE server, the switch port is assigned the dynamic VLAN as shown below in the output of the show command on R1.

```
admin@R1# run show dot1x interface gigabit-ethernet te-1/1/20
Interface ge-1/1/20:
===============================================================
Client MAC : cc:98:91:4e:c9:a7
Status : authorized
Success Auth Method : MAB
Traffic Class : Other
Dynamic VLAN ID : 20 (active)
===============================================================
```

On R1 run the command **run show route vrf vrf1** to display the routes. Notice below that there is a route to subnet 30.1.1.0/24.

```
admin@R1# run show route vrf vrf1
show ip route vrf vrf1
======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 04:07:17
C>* 10.1.1.0/24 is directly connected, vlan10, 04:06:28
C>* 20.1.1.0/24 is directly connected, vlan20, 04:05:33
B>* 11.11.11.147/32 [200/0] via 2.2.2.2, vlan1111 onlink, weight 1, 04:05:30
C>* 30.1.1.0/24 is directly connected, vlan30, 04:06:28
C>* 201.201.201.201/32 is directly connected, vrf1, 04:07:17



show ipv6 route vrf vrf1
========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
C * fe80::/64 is directly connected, vlan1111, 04:06:27
C * fe80::/64 is directly connected, vlan30, 04:06:28
C>* fe80::/64 is directly connected, vlan10, 04:06:28
```

```
admin@R2# run show route vrf vrf1
show ip route vrf vrf1
======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:12:12
C>* 10.1.1.0/24 is directly connected, vlan10, 00:11:23
C>* 20.1.1.0/24 is directly connected, vlan10, 00:11:33
C>* 30.1.1.0/24 is directly connected, vlan30, 00:11:23
```

```
show ipv6 route vrf vrf1
=========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
C * fe80::/64 is directly connected, vlan1111, 00:11:22
C * fe80::/64 is directly connected, vlan30, 00:11:22
C * fe80::/64 is directly connected, vlan10, 00:11:22
C>* fe80::/64 is directly connected, vlan40, 00:11:22
```

Run the command **run show vxlan evpn route** on either R1 or R2 to check the VXLAN EVPN routes.

```
admin@R1#  run show vxlan arp
IP-ADDRESS       MAC-ADDRESS         VNI       Status       Age       Interface   REMOTE-VTEP
---------------  -----------------  --------  --------     -------    ----------   ----------
10.1.1.2        18:5a:58:3c:42:a1  10         Dynamic      249        te-1/1/10
20.1.1.1        17:54:56:ac:42:22  20         Dynamic      250        te-1/1/20
10.1.1.1        18:5a:58:03:35:81  10         Static                              2.2.2.2
30.1.1.1        18:5a:58:03:35:81  30         Static                              2.2.2.2
30.1.1.2        1c:72:1d:c9:1b:e1  30         Static                              2.2.2.2
```

To check the VXLAN tunnels on either devices, run the command **run show vxlan tunnel.**

```
admin@R2# run show vxlan tunnel
Total number of tunnels: 3

VNI 10, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 20, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 30, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 100, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1
```

EVPN Multihoming Configuration Guide

- Introduction
  - Key Benefits
  - Brief Mechanism
    - EVPN Type-1 Ethernet Auto Discovery (A-D) Route
    - EVPN Type-4 Ethernet Segment Route
  - Designated Forwarder Election
  - VTEP Uplink Status Tracking
  - EVPN MH Split Horizon
  - EVPN MH Basic Configuration
  - Aliasing
- Switch Configuration Example and Topology
  - EVPN Multihoming with Head End Replication
    - Leaf1 Configuration
    - Leaf2 Configuration
    - Leaf3 Configuration
    - Leaf4 Configuration
    - Spine1 Configuration
    - Spine2 Configuration
    - Verify Configuration
  - EVPN Multihoming with BUM Tunnel
    - Leaf1 Configuration
    - Leaf2 Configuration
    - Leaf3 Configuration
    - Leaf4 Configuration
    - Spine1 Configuration
    - Spine2 Configuration
    - Verify Configuration

Introduction

EVPN Multihoming (MH) is a standards based replacement for MLAG to achieve standards based all-active server redundancy in datacenters and enterprise networks. Multihoming eliminates the need to have MLAG and unlike MLAG, does not require the group of devices used to create a multihoming group to have inter-connecting peer links.

EVPN multihoming is based on the concept of forming Ethernet Segments (ES). In the context of BGP EVPN, an Ethernet Segment is a set of links connecting a single end host or server with the EVPN VXLAN fabric. In the Figure below, Server1 is multihomed to the VXLAN fabric through links connecting it to VTEP1 and VTEP2, forming an Ethernet Segment. Similarly, Server2, Server3 and Server4 are connected to the fabric through links forming segment 2, segment 3 and segment 4 respectively.

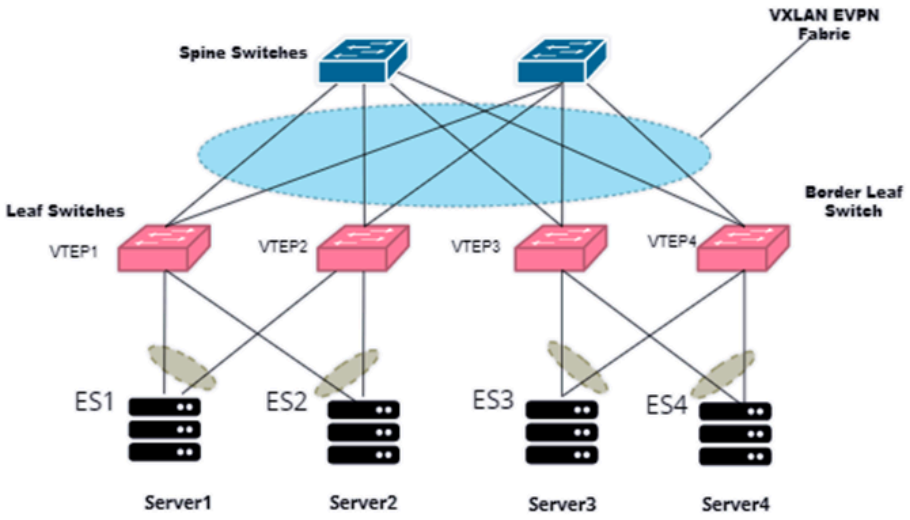


Figure 1. EVPN Multihoming

Key Benefits

- Interconnecting switch links between TOR switches in a redundancy group are not required.
- There can be more than two TOR switches in the redundancy group. A maximum of 8 devices can form one redundancy group as opposed to a maximum of two devices in an MLAG group.
- Ease of management as it provides a single BGP-EVPN control plane.
- Allows multi-vendor interoperability because of standards based implementation.

Brief Mechanism

As shown in Figure 1, if VTEP1 loses direct connection to Server1, it will signal to VTEP2, VTEP3 and VTEP4 that Server1 is no longer accessible and to change their next-hop group for Server1 if there are alternative routes to this ES. Since VTEP2 also has a route to this ES, VTEP3 and VTEP4 will change their next hop groups for Server1 MAC address to go through VTEP2 instead of VTEP1.

EVPN multihoming uses EVPN Type-1, Type-2 and Type-4 routes to discover these Ethernet Segments and deliver traffic to and from these segments. Each Ethernet Segment is identified by a unique ID called Ethernet Segment ID (ESI). ESI is unique across the entire EVPN VXLAN domain on all VTEPs. To configure ESI, we first need to configure the Ethernet Segment System MAC and a local ES-ID. The local ES system MAC and local ES ID are used to automatically generate the ESI. Different ES System MACs can be configured for different Ethernet Segments but the ES System MAC configured on interfaces connecting to the same server or host must be same. In the sections below we will briefly explore EVPN Type-1Auto Discovery and EVPN Type-4 Ethernet Segment Routes.

EVPN Type-1 Ethernet Auto Discovery (A-D) Route

EVPN Type-1 routes are used for fast convergence and aliasing for multihomed sites or end hosts. Fast convergence is important in networks with large number of hosts. When a link failure occurs, devices can signal to upstream PE devices or other VTEPs in the network to change their next-hop groups for the MAC addresses associated with that particular Ethernet Segment. Aliasing is used for load balancing on multiple outgoing links.

Route Distinguisher (RD) (8 octets)
Ethernet Segment Identifier (10 octets)
Ethernet Tag ID (4 octets)
MPLS Label (3 octets)

Table 1. EVPN Type-1 Route NLRI

Type-1 routes are only originated for multihomed devices, i.e. these routes are sent only when the Ethernet Segment ID is set to a non-zero value.

EVPN Type-4 Ethernet Segment Route

Type-4 routes are used for electing the Designated Forwarder (DF) in EVPN multihoming scenarios. The DF is responsible for sending broadcast, unknown unicast and multicast (BUM) traffic to multihomed hosts or servers. If a server is multihomed to two upstream devices in the EVPN fabric, only one would be elected as the DF for sending BUM traffic to the multihomed server on this ES.

The EVPN NLRI for Type-4 Ethernet Segment Route consists of the following four fields. For multihomed hosts, the Ethernet Segment Identifier (ESI) must be set to a non-zero value. A value of zero for the ESI indicates a single homed device.

RD (8 Octets)
Ethernet Segment Identifier (10 Octets)
IP Address Length (1 octet)
Originating Router's IP Address (4 or 16 octets)

Table 2. EVPN Type-4 NLRI

EVPN multihoming works by utilizing EVPN Type-1, Type-2 and Type-4 routes. Three types of EVPN routes are used to fulfill three distinct EVPN multihoming requirements.

The PICOS EVPN multihoming can be summarized in the following three steps

Step1:

EVPN Type-2 routes are used for remote learning of end hosts. As shown in Figure 1 for example, Server1 is multihomed to VTEP1 and VTEP2. Both VTEP1 and VTEP2 will first locally learn Server1's MAC/IP address and then advertise it to VTEP3 and VTEP4 using EVPN Type-2 routes (remote learning).

Step2:

With EVPN multihoming enabled on switch ports connecting Server1 to VTEP1 and VTEP2, both devices will configure the same Ethernet Subnet Identifier (ESI) on the two links and advertise this information to all the other VTEPs using Type-4 routes. This will indicate to remote VTEPs that Server1 is multihomed to the EVPN fabric and is accessible through both VTEP1 and VTEP2.

Step3:

For fast convergence and aliasing, VTEP1 and VTEP2 will advertise Type-1 routes. This type of advertisement is sent in the event of a link failure. If the link connecting VTEP1 and Server1 goes down, VTEP1 will advertise Type-1 route indicating to all the other VTEPs that it has lost connection with Server1 (Ethernet Segment). If VTEP1 was elected the

designated forward (DF) for this segment, VTEP2 will then assume the role of DF for Server1 whereas VTEP3 and VTEP4 will adjust their next-hop groups for Server1 accordingly.

> **Note**
> It is strongly suggested to remove any MLAG related configuration from the overlay devices (VTEPs) if you plan on deploying EVPN MH in your network. The two technologies are designed to address almost similar requirements of redundancy but MLAG is a layer2 technique whereas EVPN MH is deployed in the overlay and is a layer3 technique. The two technologies hence do not mix well and users are urged to stick to EVPN MH for its standards based implementation and interoperability benefits as opposed to MLAG especially in the overlay network design.

Designated Forwarder Election

For BGP EVPN, a Designated Forwarder (DF) is responsible for handling Broadcast, Unknown Unicast and Multicast (BUM) traffic for Ethernet Segments. As shown in Figure 1, Server1 constitutes an Ethernet Segment as it is multihomed to two VTEPs in the EVPN overlay. Only one of the two VTEPs has to be elected a DF to deliver BUM traffic to Server1 from remote VTEPs (VTEP3 and VTEP4). The administrator needs to configure EVPN multihoming preference for the Ethernet Segment. A higher preference value wins the election process and assumes the role of the DF. If the preference on both the VTEPs is same then the VTEP with the smallest IP wins the election. It's important to note that the interface connecting the Ethernet Segment must be an Aggregate-Ethernet interface.

For every Ethernet Segment there must be only one DF.

The following command can be used to set the ES DF preference.

set interface aggregate-ethernet <*interface*> **evpn mh es-df-pref** <*preference*>

VTEP Uplink Status Tracking

Overlay VTEPs are capable of tracking the state of uplinks connecting the overlay leaf devices with underlay spine switches. This feature is automatically enabled when the user enables the EVPN MH. All the downstream links connecting the MH hosts are put in *protocol down* state when all the uplinks go down. In Figure 1, all the links connecting the underlay spine switches must go down before the downstream links are put in *protocol down* state. The links will not be put in *protocol down* state if there is only one link up and active connecting the overlay devices with the underlay.

EVPN MH Split Horizon

Split-horizon technique is used to stop BUM traffic from forming a loop in the EVPN VXLAN network that employs multihoming. Using split-horizon, BUM traffic from the same Ethernet Segment will be dropped by the peer device. As can been seen in Figure 2, Host1 is multihomed into the EVPN VXLAN fabric and connected to both VTEP1 and VTEP2 forming Ethernet Segment ES1.

In the example below, if Host1 sends some BUM traffic to DF and then it is forwarded to the spine switch and then relayed back to VTEP2, that traffic will be discarded at VTEP2 since VTEP2 has an interface configured for the same Ethernet Segment. Split horizon mechanism ensures BUM traffic can't loop back to Host1 if Host1 originates this traffic.

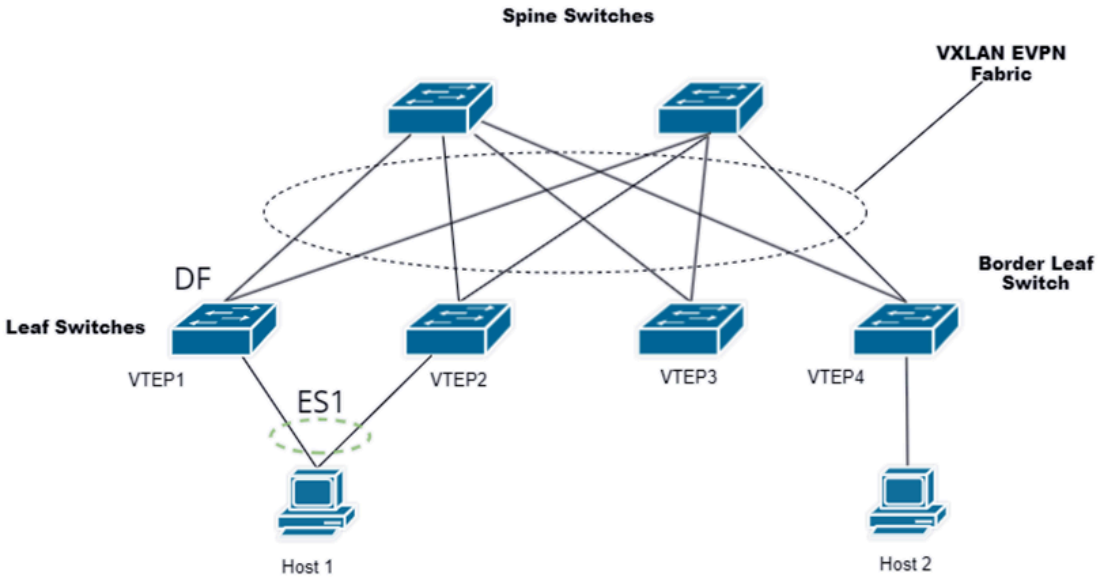


Figure 2. EVPN MH Split-Horizon

Key points to note for EVPN MH Split Horizon and BUM traffic duplication:

1. Only one DF is elected in one ESI (one LAG), so partial connection is not allowed for EVPN MH access connection.
2. Non-DF node will drop the BUM traffic from other nodes, including peer of the same ES. BUM traffic from remote VTEPs is dropped by non-DF nodes to avoid duplication.

> **Note**
> **Note:** Single homed ports connecting a single device with the EVPN VXLAN fabric are not yet supported on VTEP devices. If a server is dual homed to two VTEPs and the connecting link to one of the VTEP fails, the server will still be considered a dual homed device even if there is only one active link connecting it to the fabric.

EVPN MH Basic Configuration

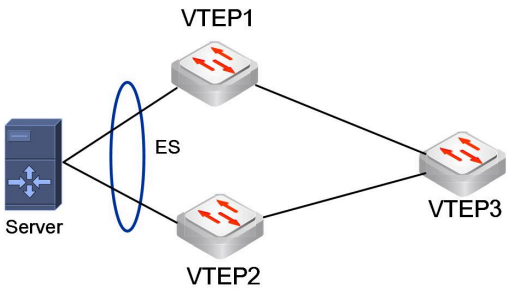
To configure EVPN multihoming on a LAG interface, the user needs to configure an Ethernet Segment identifier (ES-ID) and an Ethernet Segment System MAC. A type-3 ESI value is automatically generated by using these two parameters. The resulting 10-byte ESI value has the following format, where the XXs denote the 6-byte ES System MAC and the YYs denote the 3-byte local ES ID.

03 : XX : XX : XX : XX : XX : XX : YY : YY : YY

For each Ethernet segment, both the ES System MAC and the ES ID must be the same on all the switches forming the EVPN MH redundancy group. However, switches can be configured with different system MACs for different Ethernet segments or share the same system MAC for all Ethernet segments.

Aliasing

The aliasing feature provides remote VTEP devices the ability to load balance Layer-2 unicast traffic through other VTEPs that have configured the same ES (Ethernet Segment). VTEP devices in the EVPN multihoming redundancy group always advertise the communicated information of the same ES to all remote VTEPs via MP-BGP protocol. If one of the VTEP device in an ES, say VTEP1 in the following figure, learns the MAC/ARP information and advertises it to the remote VTEP, say VTEP3. Then, VTEP3 adds not only the IP address of VTEP1 as the next hop, but also adds the IP addresses of other VTEPs in the EVPN multihoming redundancy group as the next hop, to automatically form equivalent paths between different VTEPs.



EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:

set interface ecmp hash-mapping field ingress-interface disable

set interface ecmp hash-mapping field ip-destination disable

set interface ecmp hash-mapping field ip-protocol disable

set interface ecmp hash-mapping field ip-source disable

set interface ecmp hash-mapping field port-destination disable

set interface ecmp hash-mapping field port-source disable

set interface ecmp hash-mapping field vlan disable

On the remote VTEP, run the following EVPN MAC show commands to view the next hop. It shows the next hop interface is *vplag*, including all VTEPs in remote ES.

```
admin@Xorplus# run show mac-address table
Total entries in switching table:   1
Static entries in switching table:  0
Dynamic entries in switching table: 1

VLAN         MAC address          Type         Age     Interfaces         User
----         -----------------    ---------    ----    ----------------   ----------
N/A          00:0c:29:77:8b:15    Dynamic      300     vplag-0x1          xorp


admin@Xorplus# run show vxlan address-table
VNID          MAC address          Type          Interface          VTEP
-----------   -----------------    -------       ----------------   ---------------
10020         00:0c:29:77:8b:15    Dynamic                          10.226.14.253,10.226.14.254
Entries in access port:  0
Entries in network port: 1
```

Switch Configuration Example and Topology

In PICOS EVPN multihoming, there are two ways to forward BUM messages. You can choose one of these to apply to your EVPN fabric.

- **Head End Replication.** This is the default way which needs no PIM configurations. The BUM message will be encapsulated and sent to all outgoing ports VTEPs of the same VNI by the access VTEP.
- **BUM tunnel.** All VTEPs of the same VNI join the same multicast group, and use multicast routing protocol PIM to establish a multicast forwarding table entry for the multicast group. This method can reduce the traffic flooding caused by the head end replication of the BUM messages. This way needs to configure PIM protocol.

EVPN Multihoming with Head End Replication

For this example configuration we have the following topology comprising of two spine switches, four leaf switches and four servers that are multihomed to this network. Two servers are multihomed to Leaf1 and Leaf2 switches whereas the other two servers are attached to Leaf3 and Leaf4 switches.

The four leaf switches form two MH redundancy groups for the four ES IDs. Two ES ID's are configured under Leaf1 and Leaf2 whereas, another two ES ID's are configured under Leaf3 and Leaf4. Each leaf switch has one physical interface added to a LAG interface to connect to the downstream server.

The two ES IDs are configured on each peer connected to the two downstream multihomed servers. On Leaf1, two physical ports connect to the multihomed servers; both the physical ports are first added to LAG interfaces. The LAG interface connected to Server1 is "ae2" whereas the interface connecting Server2 is "ae1". For EVPN MH, it is a mandatory that the ports connecting the multihomed hosts must be LAG interfaces. Similarly, on all leaf switches there are two LAG interfaces and two ES IDs configured.

To implement a seamless migration of VMs without changing network settings or disrupting the traffic forwarding, configure the same anycast gateway IP and the same virtual MAC (router MAC) on all four leaf switches to enable the anycast gateway function.

The following configuration examples use the topology illustrated below and configure EVPN multihoming with head end replication.

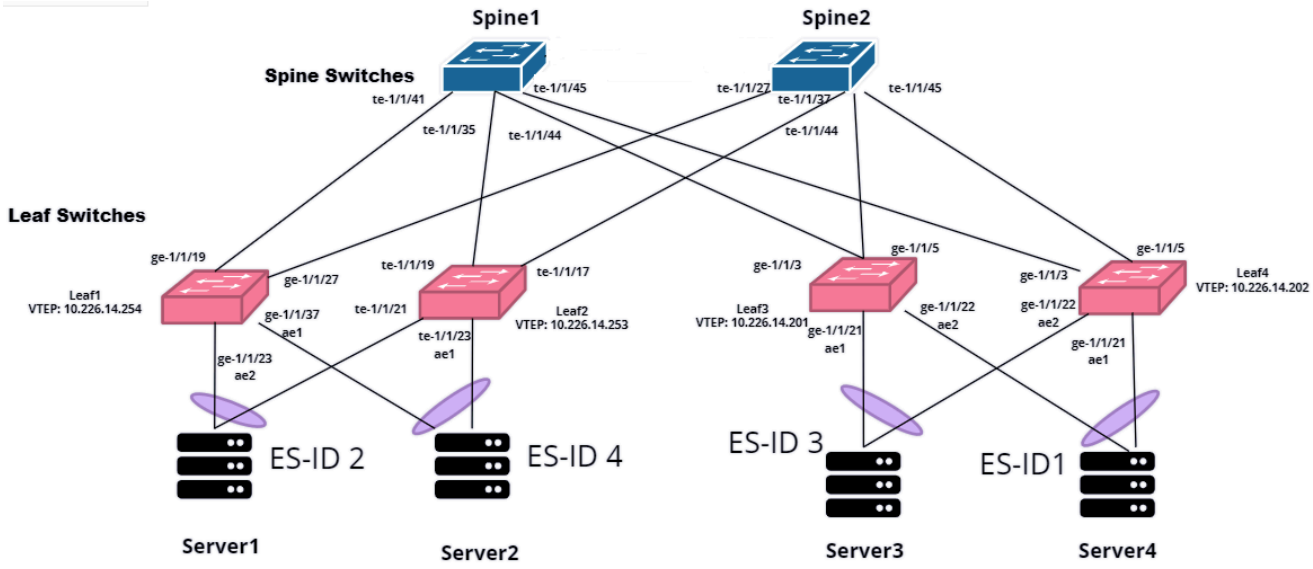


Figure 3. EVPN MH Example Topology

> **Note**
> **Note:** The physical ports connecting the multihomed servers or hosts must be added to a LAG interface and then configured for EVPN MH. Physical interfaces such as ge-1/1/1 cannot be directly used for MH configuration.

Leaf1 Configuration

Step 1. Configure LAG interfaces, set the LAG interface MTU, configure ES ID, configure the LAG interface VLAN membership and the LAG interface trunk mode. MTU configuration is optional, it can be configured when the MTU size needs to be of a particular size based on the customer use case environment. The LACP configuration is also optional.

```
admin@Leaf1# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Leaf1# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
admin@Leaf1# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Leaf1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 30
admin@Leaf1# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Leaf1# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@Leaf1# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 30
admin@Leaf1# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 20
admin@Leaf1# set interface aggregate-ethernet ae1 evpn mh es-id 4
admin@Leaf1# set interface aggregate-ethernet ae2 evpn mh es-id 2
```

Step2. Configure ES system MAC, it can be the same or different for different ethernet segments. Configure the physical interfaces and VLAN membership and the ports trunk mode. Also add physical interfaces to LAG interfaces.

```
admin@Leaf1# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Leaf1# set interface aggregate-ethernet ae2 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Leaf1# set interface gigabit-ethernet ge-1/1/19 mtu 3000
admin@Leaf1# set interface gigabit-ethernet ge-1/1/19 family ethernet-switching native-vlan-id 4014
admin@Leaf1# set interface gigabit-ethernet ge-1/1/23 ether-options 802.3ad ae2
admin@Leaf1# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching
admin@Leaf1# set interface gigabit-ethernet ge-1/1/24 disable true
admin@Leaf1# set interface gigabit-ethernet ge-1/1/27 mtu 3000
```

```
admin@Leaf1# set interface gigabit-ethernet ge-1/1/27 family ethernet-switching native-vlan-id 4012
admin@Leaf1# set interface gigabit-ethernet ge-1/1/37 ether-options 802.3ad ae1
```

Step3. Configure VRF and enable IP routing.

```
admin@Leaf1# set ip routing enable true
admin@Leaf1# set ip vrf vrf1
```

Step4. Configure loopback interfaces and assign IP addresses.

```
admin@Leaf1# set l3-interface loopback lo address 10.226.14.254 prefix-length 32
admin@Leaf1# set l3-interface loopback lo address 10.226.14.207 prefix-length 32
admin@Leaf1# set l3-interface loopback vrf1 address 17.17.17.17 prefix-length 32
```

Step5. Configure VLAN interfaces and assign IP addresses, configure anycast gateway.

```
admin@Leaf1# set l3-interface vlan-interface vlan4014 address 10.226.15.65 prefix-length 30
admin@Leaf1# set l3-interface vlan-interface vlan4012 address 10.226.15.29 prefix-length 30
admin@Leaf1# set l3-interface vlan-interface vlan4094 address 10.226.13.26 prefix-length 30
admin@Leaf1# set l3-interface vlan-interface vlan99 vrf vrf1
admin@Leaf1# set l3-interface vlan-interface vlan20 vrf vrf1
admin@Leaf1# set l3-interface vlan-interface vlan20 address 192.168.0.1 prefix-length 24
admin@Leaf1# set l3-interface vlan-interface vlan20 address 2002:0:0:1::1 prefix-length 64
admin@Leaf1# set l3-interface vlan-interface vlan30 vrf vrf1
admin@Leaf1# set l3-interface vlan-interface vlan30 address 172.168.0.1 prefix-length 24
admin@Leaf1# set l3-interface vlan-interface vlan30 address 2003:0:0:1::1 prefix-length 64
admin@Leaf1# set l3-interface vlan-interface vlan20 anycast address 192.168.0.20 prefix-length 24
admin@Leaf1# set l3-interface vlan-interface vlan20 anycast address 2002:0:0:1::20 prefix-length 64
admin@Leaf1# set l3-interface vlan-interface vlan30 anycast address 172.168.0.30 prefix-length 24
admin@Leaf1# set l3-interface vlan-interface vlan30 anycast address 2003:0:0:1::30 prefix-length 64
admin@Leaf1# set l3-interface vlan-interface vlan20 anycast mac 00:00:20:00:00:FE
admin@Leaf1# set l3-interface vlan-interface vlan30 anycast mac 00:00:30:00:00:FE
```

Step6. Configure BGP and EVPN.

```
admin@Leaf1# set protocols bgp local-as 65001
admin@Leaf1# set protocols bgp router-id 10.226.14.207
admin@Leaf1# set protocols bgp neighbor 10.226.14.48 remote-as internal
admin@Leaf1# set protocols bgp neighbor 10.226.14.48 update-source 10.226.14.207
admin@Leaf1# set protocols bgp neighbor 10.226.14.48 evpn activate true
admin@Leaf1# set protocols bgp neighbor 10.226.14.208 remote-as internal
admin@Leaf1# set protocols bgp neighbor 10.226.14.208 update-source 10.226.14.207
admin@Leaf1# set protocols bgp neighbor 10.226.14.208 evpn activate true
admin@Leaf1# set protocols bgp neighbor 10.226.14.24 remote-as internal
admin@Leaf1# set protocols bgp neighbor 10.226.14.24 update-source 10.226.14.207
admin@Leaf1# set protocols bgp neighbor 10.226.14.24 evpn activate true
admin@Leaf1# set protocols bgp ipv4-unicast
admin@Leaf1# set protocols bgp evpn advertise-all-vni
admin@Leaf1# set protocols bgp evpn advertise ipv4-unicast
admin@Leaf1# set protocols bgp evpn advertise ipv6-unicast
admin@Leaf1# set protocols bgp evpn advertise-svi-ip
admin@Leaf1# set protocols bgp vrf vrf1 local-as 65001
admin@Leaf1# set protocols bgp vrf vrf1 router-id 17.17.17.17
admin@Leaf1# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@Leaf1# set protocols bgp vrf vrf1 evpn advertise ipv6-unicast
admin@Leaf1# set protocols evpn mh
admin@Leaf1# set protocols lldp enable true
```

Step7. Configure OSPF.

```
admin@Leaf1# set protocols ospf router-id 17.17.17.17
admin@Leaf1# set protocols ospf network 10.226.15.64/30 area 0.0.0.0
admin@Leaf1# set protocols ospf network 10.226.15.28/30 area 0.0.0.0
admin@Leaf1# set protocols ospf network 10.226.14.254/32 area 0.0.0.0
admin@Leaf1# set protocols ospf network 10.226.14.207/32 area 0.0.0.0
```

Step8. Configure hostname, inband mode and VLANs.

```
admin@Leaf1# set system hostname Leaf1
admin@Leaf1# set system inband enable true
admin@Leaf1# set vlans vlan-id 20 l3-interface vlan20
admin@Leaf1# set vlans vlan-id 30 l3-interface vlan30
admin@Leaf1# set vlans vlan-id 99 l3-interface vlan99
admin@Leaf1# set vlans vlan-id 4012 l3-interface vlan4012
admin@Leaf1# set vlans vlan-id 4014 l3-interface vlan4014
admin@Leaf1# set vlans vlan-id 4094 l3-interface vlan4094
```

Step9. Configure VXLANs.

```
admin@Leaf1# set vxlans source-interface lo address 10.226.14.254
admin@Leaf1# set vxlans vni 10030 decapsulation mode service-vlan-per-port
admin@Leaf1# set vxlans vni 10030 vlan 30
admin@Leaf1# set vxlans vni 10030 arp-nd-suppress disable false
admin@Leaf1# set vxlans vni 10020 decapsulation mode service-vlan-per-port
admin@Leaf1# set vxlans vni 10020 vlan 20
admin@Leaf1# set vxlans vni 10020 arp-nd-suppress disable false
admin@Leaf1# set vxlans vni 99 vlan 99
admin@Leaf1# set vxlans vrf vrf1 l3-vni 99
admin@Leaf1# commit
```

Leaf2 Configuration

```
admin@Leaf2# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Leaf2# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
admin@Leaf2# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Leaf2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 30
admin@Leaf2# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Leaf2# set interface aggregate-ethernet ae1 evpn mh es-id 4
admin@Leaf2# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Leaf2# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@Leaf2# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 30
admin@Leaf2# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 20
admin@Leaf2# set interface aggregate-ethernet ae2 evpn mh es-id 2
admin@Leaf2# set interface aggregate-ethernet ae2 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Leaf2# set interface gigabit-ethernet te-1/1/17 mtu 3000
admin@Leaf2# set interface gigabit-ethernet te-1/1/17 family ethernet-switching native-vlan-id 4014
admin@Leaf2# set interface gigabit-ethernet te-1/1/19 mtu 3000
admin@Leaf2# set interface gigabit-ethernet te-1/1/19 family ethernet-switching native-vlan-id 4013
admin@Leaf2# set interface gigabit-ethernet te-1/1/21 ether-options 802.3ad ae2
admin@Leaf2# set interface gigabit-ethernet te-1/1/23 ether-options 802.3ad ae1
admin@Leaf2# set interface ethernet-switching-options
admin@Leaf2# set ip routing enable true
admin@Leaf2# set ip vrf vrf1
admin@Leaf2# set l3-interface loopback lo address 10.226.14.253 prefix-length 32
admin@Leaf2# set l3-interface loopback vrf1 address 26.26.26.26 prefix-length 32
admin@Leaf2# set l3-interface vlan-interface vlan4013 address 10.226.15.25 prefix-length 30
admin@Leaf2# set l3-interface vlan-interface vlan4014 address 10.226.15.81 prefix-length 30
admin@Leaf2# set l3-interface vlan-interface vlan4094 address 10.226.13.25 prefix-length 30
admin@Leaf2# set l3-interface vlan-interface vlan99 vrf vrf1
admin@Leaf2# set l3-interface vlan-interface vlan20 vrf vrf1
admin@Leaf2# set l3-interface vlan-interface vlan20 address 192.168.0.2 prefix-length 24
admin@Leaf2# set l3-interface vlan-interface vlan20 address 2002:0:0:1::2 prefix-length 64
admin@Leaf2# set l3-interface vlan-interface vlan30 vrf vrf1
admin@Leaf2# set l3-interface vlan-interface vlan30 address 172.168.0.2 prefix-length 24
admin@Leaf2# set l3-interface vlan-interface vlan30 address 2003:0:0:1::2 prefix-length 64
admin@Leaf2# set l3-interface vlan-interface vlan20 anycast address 192.168.0.20 prefix-length 24
admin@Leaf2# set l3-interface vlan-interface vlan20 anycast address 2002:0:0:1::20 prefix-length 64
admin@Leaf2# set l3-interface vlan-interface vlan30 anycast address 172.168.0.30 prefix-length 24
admin@Leaf2# set l3-interface vlan-interface vlan30 anycast address 2003:0:0:1::30 prefix-length 64
admin@Leaf2# set l3-interface vlan-interface vlan20 anycast mac 00:00:20:00:00:FE
admin@Leaf2# set l3-interface vlan-interface vlan30 anycast mac 00:00:30:00:00:FE
admin@Leaf2# set protocols bgp local-as 65001
admin@Leaf2# set protocols bgp router-id 10.226.14.208
admin@Leaf2# set protocols bgp neighbor 10.226.14.48 remote-as internal
admin@Leaf2# set protocols bgp neighbor 10.226.14.48 update-source 10.226.14.208
```

```
admin@Leaf2# set protocols bgp neighbor 10.226.14.48 evpn activate true
admin@Leaf2# set protocols bgp neighbor 10.226.14.207 remote-as internal
admin@Leaf2# set protocols bgp neighbor 10.226.14.207 update-source 10.226.14.208
admin@Leaf2# set protocols bgp neighbor 10.226.14.207 evpn activate true
admin@Leaf2# set protocols bgp neighbor 10.226.14.24 remote-as internal
admin@Leaf2# set protocols bgp neighbor 10.226.14.24 update-source 10.226.14.208
admin@Leaf2# set protocols bgp neighbor 10.226.14.24 evpn activate true
admin@Leaf2# set protocols bgp ipv4-unicast
admin@Leaf2# set protocols bgp evpn advertise-all-vni
admin@Leaf2# set protocols bgp evpn advertise ipv4-unicast
admin@Leaf2# set protocols bgp evpn advertise ipv6-unicast
admin@Leaf2# set protocols bgp evpn advertise-svi-ip
admin@Leaf2# set protocols bgp vrf vrf1 local-as 65001
admin@Leaf2# set protocols bgp vrf vrf1 router-id 26.26.26.26
admin@Leaf2# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@Leaf2# set protocols bgp vrf vrf1 evpn advertise ipv6-unicast
admin@Leaf2# set protocols evpn mh
admin@Leaf2# set protocols lldp enable true
admin@Leaf2# set protocols ospf router-id 110.110.110.110
admin@Leaf2# set protocols ospf network 10.226.15.24/30 area 0.0.0.0
admin@Leaf2# set protocols ospf network 10.226.15.80/30 area 0.0.0.0
admin@Leaf2# set protocols ospf network 10.226.14.208/32 area 0.0.0.0
admin@Leaf2# set protocols ospf network 10.226.14.253/32 area 0.0.0.0
admin@Leaf2# set vlans vlan-id 20 l3-interface vlan20
admin@Leaf2# set vlans vlan-id 30 l3-interface vlan30
admin@Leaf2# set vlans vlan-id 99 l3-interface vlan99
admin@Leaf2# set vlans vlan-id 4013 l3-interface vlan4013
admin@Leaf2# set vlans vlan-id 4014 l3-interface vlan4014
admin@Leaf2# set vlans vlan-id 4094 l3-interface vlan4094
admin@Leaf2# set vxlans source-interface lo address 10.226.14.253
admin@Leaf2# set vxlans vni 10030 decapsulation mode service-vlan-per-port
admin@Leaf2# set vxlans vni 10030 vlan 30
admin@Leaf2# set vxlans vni 10030 arp-nd-suppress disable false
admin@Leaf2# set vxlans vni 10020 decapsulation mode service-vlan-per-port
admin@Leaf2# set vxlans vni 10020 vlan 20
admin@Leaf2# set vxlans vni 10020 arp-nd-suppress disable false
admin@Leaf2# set vxlans vni 99 vlan 99
admin@Leaf2# set vxlans vrf vrf1 l3-vni 99
admin@Leaf2# commit
```

Leaf3 Configuration

```
admin@Leaf3# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Leaf3# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
admin@Leaf3# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Leaf3# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 30
admin@Leaf3# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Leaf3# set interface aggregate-ethernet ae1 evpn mh es-id 3
admin@Leaf3# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:00:00:22:22:22
admin@Leaf3# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@Leaf3# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 30
admin@Leaf3# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 20
admin@Leaf3# set interface aggregate-ethernet ae2 evpn mh es-id 1
admin@Leaf3# set interface aggregate-ethernet ae2 evpn mh es-sys-mac 00:00:00:22:22:22
admin@Leaf3# set interface gigabit-ethernet ge-1/1/3 mtu 3000
admin@Leaf3# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3011
admin@Leaf3# set interface gigabit-ethernet ge-1/1/5 mtu 3000
admin@Leaf3# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 3012
admin@Leaf3# set interface gigabit-ethernet ge-1/1/21 ether-options 802.3ad ae1
admin@Leaf3# set interface gigabit-ethernet ge-1/1/22 ether-options 802.3ad ae2
admin@Leaf3# set interface ethernet-switching-options
admin@Leaf3# set ip routing enable true
admin@Leaf3# set ip vrf vrf1
admin@Leaf3# set l3-interface loopback lo address 10.226.14.24 prefix-length 32
admin@Leaf3# set l3-interface loopback lo address 10.226.14.201 prefix-length 32
admin@Leaf3# set l3-interface vlan-interface vlan3011 address 10.226.0.98 prefix-length 30
admin@Leaf3# set l3-interface vlan-interface vlan3012 address 10.226.0.94 prefix-length 30
admin@Leaf3# set l3-interface vlan-interface vlan99 vrf vrf1
admin@Leaf3# set l3-interface vlan-interface vlan20 vrf vrf1
```

```
admin@Leaf3# set l3-interface vlan-interface vlan20 address 192.168.0.3 prefix-length 24
admin@Leaf3# set l3-interface vlan-interface vlan20 address 2002:0:0:1::3 prefix-length 64
admin@Leaf3# set l3-interface vlan-interface vlan30 vrf vrf1
admin@Leaf3# set l3-interface vlan-interface vlan30 address 172.168.0.3 prefix-length 24
admin@Leaf3# set l3-interface vlan-interface vlan30 address 2003:0:0:1::3 prefix-length 64
admin@Leaf3# set l3-interface vlan-interface vlan20 anycast address 192.168.0.20 prefix-length 24
admin@Leaf3# set l3-interface vlan-interface vlan20 anycast address 2002:0:0:1::20 prefix-length 64
admin@Leaf3# set l3-interface vlan-interface vlan30 anycast address 172.168.0.30 prefix-length 24
admin@Leaf3# set l3-interface vlan-interface vlan30 anycast address 2003:0:0:1::30 prefix-length 64
admin@Leaf3# set l3-interface vlan-interface vlan20 anycast mac 00:00:20:00:00:FE
admin@Leaf3# set l3-interface vlan-interface vlan30 anycast mac 00:00:30:00:00:FE
admin@Leaf3# set protocols bgp local-as 65001
admin@Leaf3# set protocols bgp router-id 10.226.14.24
admin@Leaf3# set protocols bgp neighbor 10.226.14.207 remote-as internal
admin@Leaf3# set protocols bgp neighbor 10.226.14.207 timers delayopen 60
admin@Leaf3# set protocols bgp neighbor 10.226.14.207 update-source 10.226.14.24
admin@Leaf3# set protocols bgp neighbor 10.226.14.207 evpn activate true
admin@Leaf3# set protocols bgp neighbor 10.226.14.208 remote-as internal
admin@Leaf3# set protocols bgp neighbor 10.226.14.208 timers delayopen 60
admin@Leaf3# set protocols bgp neighbor 10.226.14.208 update-source 10.226.14.24
admin@Leaf3# set protocols bgp neighbor 10.226.14.208 evpn activate true
admin@Leaf3# set protocols bgp neighbor 10.226.14.48 remote-as internal
admin@Leaf3# set protocols bgp neighbor 10.226.14.48 timers delayopen 60
admin@Leaf3# set protocols bgp neighbor 10.226.14.48 update-source 10.226.14.24
admin@Leaf3# set protocols bgp neighbor 10.226.14.48 evpn activate true
admin@Leaf3# set protocols bgp ipv4-unicast
admin@Leaf3# set protocols bgp evpn advertise-all-vni
admin@Leaf3# set protocols bgp evpn advertise ipv4-unicast
admin@Leaf3# set protocols bgp evpn advertise ipv6-unicast
admin@Leaf3# set protocols bgp evpn advertise-svi-ip
admin@Leaf3# set protocols lldp enable true
admin@Leaf3# set protocols ospf router-id 24.24.24.24
admin@Leaf3# set protocols ospf network 10.226.0.96/30 area 0.0.0.0
admin@Leaf3# set protocols ospf network 10.226.0.92/30 area 0.0.0.0
admin@Leaf3# set protocols ospf network 10.226.14.201/32 area 0.0.0.0
admin@Leaf3# set protocols ospf network 10.226.14.24/32 area 0.0.0.0
admin@Leaf3# set vlans vlan-id 20 l3-interface vlan20
admin@Leaf3# set vlans vlan-id 30 l3-interface vlan30
admin@Leaf3# set vlans vlan-id 99 l3-interface vlan99
admin@Leaf3# set vlans vlan-id 3012 l3-interface vlan3012
admin@Leaf3# set vlans vlan-id 3011 l3-interface vlan3011
admin@Leaf3# set vxlans source-interface lo address 10.226.14.201
admin@Leaf3# set vxlans vni 10020 decapsulation mode service-vlan-per-port
admin@Leaf3# set vxlans vni 10020 vlan 20
admin@Leaf3# set vxlans vni 10020 arp-nd-suppress disable false
admin@Leaf3# set vxlans vni 10030 decapsulation mode service-vlan-per-port
admin@Leaf3# set vxlans vni 10030 vlan 30
admin@Leaf3# set vxlans vni 10030 arp-nd-suppress disable false
admin@Leaf3# set vxlans vni 99 vlan 99
admin@Leaf3# set vxlans traceoptions flag all disable false
admin@Leaf3# set vxlans vrf vrf1 l3-vni 99
admin@Leaf3# commit
```

Leaf4 Configuration

```
admin@Leaf4# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@Leaf4# set interface aggregate-ethernet ae2 aggregated-ether-options lacp enable true
admin@Leaf4# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@Leaf4# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 30
admin@Leaf4# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 20
admin@Leaf4# set interface aggregate-ethernet ae1 evpn mh es-id 1
admin@Leaf4# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:00:00:22:22:22
admin@Leaf4# set interface aggregate-ethernet ae2 mtu 3000
admin@Leaf4# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@Leaf4# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 30
admin@Leaf4# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 20
admin@Leaf4# set interface aggregate-ethernet ae2 evpn mh es-id 3
admin@Leaf4# set interface aggregate-ethernet ae2 evpn mh es-sys-mac 00:00:00:22:22:22
admin@Leaf4# set interface gigabit-ethernet ge-1/1/3 mtu 3000
```

```
admin@Leaf4# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3011
admin@Leaf4# set interface gigabit-ethernet ge-1/1/5 mtu 3000
admin@Leaf4# set interface gigabit-ethernet ge-1/1/5 family ethernet-switching native-vlan-id 3012
admin@Leaf4# set interface gigabit-ethernet ge-1/1/21 ether-options 802.3ad ae1
admin@Leaf4# set interface gigabit-ethernet ge-1/1/22 ether-options 802.3ad ae2
admin@Leaf4# set ip routing enable true
admin@Leaf4# set ip vrf vrf1
admin@Leaf4# set l3-interface loopback lo address 10.226.14.202 prefix-length 32
admin@Leaf4# set l3-interface loopback lo address 10.226.14.48 prefix-length 32
admin@Leaf4# set l3-interface loopback vrf1 address 48.48.48.48 prefix-length 32
admin@Leaf4# set l3-interface vlan-interface vlan3011 address 10.226.15.70 prefix-length 30
admin@Leaf4# set l3-interface vlan-interface vlan3012 address 10.226.15.78 prefix-length 30
admin@Leaf4# set l3-interface vlan-interface vlan99 vrf vrf1
admin@Leaf4# set l3-interface vlan-interface vlan20 vrf vrf1
admin@Leaf4# set l3-interface vlan-interface vlan20 address 192.168.0.4 prefix-length 24
admin@Leaf4# set l3-interface vlan-interface vlan20 address 2002:0:0:1::4 prefix-length 64
admin@Leaf4# set l3-interface vlan-interface vlan30 vrf vrf1
admin@Leaf4# set l3-interface vlan-interface vlan30 address 172.168.0.4 prefix-length 24
admin@Leaf4# set l3-interface vlan-interface vlan30 address 2003:0:0:1::4 prefix-length 64
admin@Leaf4# set l3-interface vlan-interface vlan20 anycast address 192.168.0.20 prefix-length 24
admin@Leaf4# set l3-interface vlan-interface vlan20 anycast address 2002:0:0:1::20 prefix-length 64
admin@Leaf4# set l3-interface vlan-interface vlan30 anycast address 172.168.0.30 prefix-length 24
admin@Leaf4# set l3-interface vlan-interface vlan30 anycast address 2003:0:0:1::30 prefix-length 64
admin@Leaf4# set l3-interface vlan-interface vlan20 anycast mac 00:00:20:00:00:FE
admin@Leaf4# set l3-interface vlan-interface vlan30 anycast mac 00:00:30:00:00:FE
admin@Leaf4# set protocols bgp local-as 65001
admin@Leaf4# set protocols bgp router-id 10.226.14.48
admin@Leaf4# set protocols bgp neighbor 10.226.14.207 remote-as internal
admin@Leaf4# set protocols bgp neighbor 10.226.14.207 update-source 10.226.14.48
admin@Leaf4# set protocols bgp neighbor 10.226.14.207 evpn activate true
admin@Leaf4# set protocols bgp neighbor 10.226.14.208 remote-as internal
admin@Leaf4# set protocols bgp neighbor 10.226.14.208 update-source 10.226.14.48
admin@Leaf4# set protocols bgp neighbor 10.226.14.208 evpn activate true
admin@Leaf4# set protocols bgp neighbor 10.226.14.24 remote-as internal
admin@Leaf4# set protocols bgp neighbor 10.226.14.24 update-source 10.226.14.48
admin@Leaf4# set protocols bgp neighbor 10.226.14.24 evpn activate true
admin@Leaf4# set protocols bgp ipv4-unicast
admin@Leaf4# set protocols bgp evpn advertise-all-vni
admin@Leaf4# set protocols bgp evpn advertise ipv4-unicast
admin@Leaf4# set protocols bgp evpn advertise ipv6-unicast
admin@Leaf4# set protocols bgp evpn advertise-svi-ip
admin@Leaf4# set protocols bgp vrf vrf1 local-as 65001
admin@Leaf4# set protocols bgp vrf vrf1 router-id 48.48.48.48
admin@Leaf4# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@Leaf4# set protocols bgp vrf vrf1 evpn advertise ipv6-unicast
admin@Leaf4# set protocols evpn mh startup-delay 60
admin@Leaf4# set protocols lldp enable true
admin@Leaf4# set protocols ospf router-id 48.48.48.48
admin@Leaf4# set protocols ospf network 10.226.14.202/32 area 0.0.0.0
admin@Leaf4# set protocols ospf network 10.226.14.48/32 area 0.0.0.0
admin@Leaf4# set protocols ospf network 10.226.15.68/30 area 0.0.0.0
admin@Leaf4# set protocols ospf network 10.226.15.76/30 area 0.0.0.0
admin@Leaf4# set vlans vlan-id 20 l3-interface vlan20
admin@Leaf4# set vlans vlan-id 30 l3-interface vlan30
admin@Leaf4# set vlans vlan-id 99 l3-interface vlan99
admin@Leaf4# set vlans vlan-id 3011 l3-interface vlan3011
admin@Leaf4# set vlans vlan-id 3012 l3-interface vlan3012
admin@Leaf4# set vxlans source-interface lo address 10.226.14.202
admin@Leaf4# set vxlans vni 10020 decapsulation mode service-vlan-per-port
admin@Leaf4# set vxlans vni 10020 vlan 20
admin@Leaf4# set vxlans vni 10020 arp-nd-suppress disable false
admin@Leaf4# set vxlans vni 10030 decapsulation mode service-vlan-per-port
admin@Leaf4# set vxlans vni 10030 vlan 30
admin@Leaf4# set vxlans vni 10030 arp-nd-suppress disable false
admin@Leaf4# set vxlans vni 99 vlan 99
admin@Leaf4# set vxlans vrf vrf1 l3-vni 99
admin@Leaf4# commit
```

Spine1 Configuration

```
admin@Spine1# set interface gigabit-ethernet te-1/1/35 mtu 2000
admin@Spine1# set interface gigabit-ethernet te-1/1/35 family ethernet-switching native-vlan-id 4013
admin@Spine1# set interface gigabit-ethernet te-1/1/41 mtu 2000
admin@Spine1# set interface gigabit-ethernet te-1/1/41 family ethernet-switching native-vlan-id 4014
admin@Spine1# set interface gigabit-ethernet te-1/1/44 mtu 2000
admin@Spine1# set interface gigabit-ethernet te-1/1/44 family ethernet-switching native-vlan-id 4016
admin@Spine1# set interface gigabit-ethernet te-1/1/45 family ethernet-switching native-vlan-id 4015
admin@Spine1# set ip routing enable true
admin@Spine1# set l3-interface loopback lo address 185.185.185.185 prefix-length 32
admin@Spine1# set l3-interface vlan-interface vlan4014 address 10.226.15.66 prefix-length 30
admin@Spine1# set l3-interface vlan-interface vlan4013 address 10.226.15.26 prefix-length 30
admin@Spine1# set l3-interface vlan-interface vlan4015 address 10.226.15.69 prefix-length 30
admin@Spine1# set l3-interface vlan-interface vlan4016 address 10.226.0.97 prefix-length 30
admin@Spine1# set protocols spanning-tree enable false
admin@Spine1# set protocols ospf router-id 185.185.185.185
admin@Spine1# set protocols ospf network 10.226.15.64/30 area 0.0.0.0
admin@Spine1# set protocols ospf network 10.226.15.24/30 area 0.0.0.0
admin@Spine1# set protocols ospf network 10.226.15.68/30 area 0.0.0.0
admin@Spine1# set protocols ospf network 10.226.0.96/30 area 0.0.0.0
admin@Spine1# set protocols ospf network 185.185.185.185/32 area 0.0.0.0
admin@Spine1# set vlans vlan-id 4013 l3-interface vlan4013
admin@Spine1# set vlans vlan-id 4014 l3-interface vlan4014
admin@Spine1# set vlans vlan-id 4015 l3-interface vlan4015
admin@Spine1# set vlans vlan-id 4016 l3-interface vlan4016
admin@Spine1# commit
```

Spine2 Configuration

```
admin@Spine2# set interface gigabit-ethernet te-1/1/27 mtu 2000
admin@Spine2# set interface gigabit-ethernet te-1/1/27 family ethernet-switching native-vlan-id 4012
admin@Spine2# set interface gigabit-ethernet te-1/1/27 speed 1000
admin@Spine2# set interface gigabit-ethernet te-1/1/37 mtu 2000
admin@Spine2# set interface gigabit-ethernet te-1/1/37 family ethernet-switching native-vlan-id 4014
admin@Spine2# set interface gigabit-ethernet te-1/1/37 speed 1000
admin@Spine2# set interface gigabit-ethernet te-1/1/44 speed 1000
admin@Spine2# set interface gigabit-ethernet te-1/1/44 family ethernet-switching native-vlan-id 4015
admin@Spine2# set interface gigabit-ethernet te-1/1/45 family ethernet-switching native-vlan-id 3012
admin@Spine2# set interface gigabit-ethernet te-1/1/45 speed 1000
admin@Spine2# set ip routing enable true
admin@Spine2# set l3-interface loopback lo address 202.202.202.202 prefix-length 32
admin@Spine2# set l3-interface vlan-interface vlan4012 address 10.226.15.30 prefix-length 30
admin@Spine2# set l3-interface vlan-interface vlan4014 address 10.226.15.82 prefix-length 30
admin@Spine2# set l3-interface vlan-interface vlan4015 address 10.226.0.93 prefix-length 30
admin@Spine2# set l3-interface vlan-interface vlan3012 address 10.226.15.77 prefix-length 30
admin@Spine2# set protocols lldp enable true
admin@Spine2# set protocols spanning-tree enable false
admin@Spine2# set protocols ospf router-id 202.202.202.202
admin@Spine2# set protocols ospf network 10.226.0.92/30 area 0.0.0.0
admin@Spine2# set protocols ospf network 10.226.15.28/30 area 0.0.0.0
admin@Spine2# set protocols ospf network 10.226.15.80/30 area 0.0.0.0
admin@Spine2# set protocols ospf network 10.226.15.76/30 area 0.0.0.0
admin@Spine2# set protocols ospf network 202.202.202.202/32 area 0.0.0.0
admin@Spine2# set vlans vlan-id 4012 l3-interface vlan4012
admin@Spine2# set vlans vlan-id 4014 l3-interface vlan4014
admin@Spine2# set vlans vlan-id 4015 l3-interface vlan4015
admin@Spine2# set vlans vlan-id 3012 l3-interface vlan3012
admin@Spine2# commit
```

Verify Configuration

- The above configuration uses the same default ES-DF preferences on all the three Leaf switches. The resulting effect is that the leaf switch with the smallest VTEP IP is selected as the DF. In the first EVPN MH redundancy group, Leaf2 is elected as the DF since it has the smallest VTEP IP in the group. Similarly in the second redundancy group, Leaf3 has the smallest VTEP IP and is elected the DF.

```
admin@Leaf1# run show evpn es
Type: B bypass, L local, R remote, N non-DF
```

```
ESI                             Type   ES-IF          VTEPs
03:00:22:22:22:22:22:00:00:04     LRN   ae1          10.226.14.253
03:00:22:22:22:22:22:00:00:02     LRN   ae2          10.226.14.253

admin@Leaf2# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                             Type   ES-IF          VTEPs
03:00:22:22:22:22:22:00:00:04     LR    ae1           10.226.14.254
03:00:22:22:22:22:22:00:00:02     LR    ae2           10.226.14.254

admin@Leaf3# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                              Type   ES-IF         VTEPs
03:00:00:00:22:22:22:00:00:03      LR    ae1          10.226.14.202
03:00:00:00:22:22:22:00:00:01      LR    ae2          10.226.14.202

admin@Leaf4# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                              Type   ES-IF          VTEPs
03:00:00:00:22:22:22:00:00:01      LRN    ae1          10.226.14.201
03:00:00:00:22:22:22:00:00:03      LRN    ae2          10.226.14.201
```

- Now let's change the ES-DF preference on Leaf1 to 65535 and see the output again. This time Leaf1 assumes the role of DF.

```
admin@Leaf1# set interface aggregate-ethernet ae1 evpn mh es-df-pref 65535
admin@Leaf1# set interface aggregate-ethernet ae2 evpn mh es-df-pref 65535
admin@Leaf1# commit
Commit OK.
Save done

admin@Leaf1# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                           Type   ES-IF             VTEPs
03:00:22:22:22:22:22:00:00:04     LR    ae1             10.226.14.253
03:00:22:22:22:22:22:00:00:02     LR    ae2             10.226.14.253

admin@Leaf2# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                           Type   ES-IF             VTEPs
03:00:22:22:22:22:22:00:00:04     LRN    ae1            10.226.14.254
03:00:22:22:22:22:22:00:00:02     LRN    ae2            10.226.14.254
```

- To check the EVPN ES detail information, run the following show command. This command shows important information such as ESI, Type, interface, state, DF status and the VTEPs etc.

```
admin@Leaf3# run show evpn es detail
ESI: 03:00:00:00:22:22:22:00:00:03
 Type: Local,Remote
 Interface: ae1
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
 DF status: df
 DF preference: 32767
 Nexthop group: 536870913
 VTEPs:
     10.226.14.202 df_alg: preference df_pref: 32767 nh: 268435459
ESI: 03:00:00:00:22:22:22:00:00:01
 Type: Local,Remote
 Interface: ae2
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
```

```
DF status: df
DF preference: 32767
Nexthop group: 536870914
VTEPs:
    10.226.14.202 df_alg: preference df_pref: 32767 nh: 268435459
```

- Check the VXLAN address table with the following show command.

```
admin@Leaf3# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------    ---------------
99             04:f8:f8:20:67:7b    Dynamic                        10.226.14.254
99             18:5a:58:37:55:e1    Dynamic                        10.226.14.253
10020          04:f8:f8:20:67:7b    Dynamic                        10.226.14.253,10.226.14.254
10030          22:11:11:00:00:00    Dynamic       ae1
Entries in access port:  1
Entries in network port: 3
```

- To get the tunnel information within a VNI, run the following show command.

```
admin@Leaf3# run show vxlan tunnel vni 10030
Total number of tunnels: 2

VNI 10030, Encap:service-vlan-delete, Decap:service-vlan-per-port
  src addr:10.226.14.202, dst addr:10.226.14.253, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:10.226.15.69 10.226.15.77
  output ports:ge-1/1/5 ge-1/1/3

  src addr:10.226.14.202, dst addr:10.226.14.254, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:10.226.15.69 10.226.15.77
  output ports:ge-1/1/5 ge-1/1/3
```

- To get more info on interfaces belonging to a particular VNI, run the following show command.

```
admin@Leaf3# run show vxlan vni 10030
Interface      ID             Type           Egress     Vlan ID
-----------    -----------    -----------    -------    --------
ae1            0x80000005    Access          100012     30
ae2            0x80000006    Access          100013     30
ge-1/1/23      0x80000007    Access          100014     30
ge-1/1/5       0x80000008    Network(UC)     200258
ge-1/1/5       0x8000000a    Network(MC)     100020
ge-1/1/5       0x8000000b    Network(UC)     200258
ge-1/1/5       0x8000000d    Network(MC)     100022
ge-1/1/3       0x8000000f    Network(MC)     100024
ge-1/1/3       0x80000010    Network(UC)     100017
```

- Show the VXLAN MAC address information on Leaf1.

```
admin@Leaf1# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------    ---------------
99             18:5a:58:37:55:e1    Dynamic                  10.226.14.201
99             70:3e:44:68:22:a4    Dynamic                        10.226.14.202
10020          04:f8:f8:20:67:7b    Dynamic    ae1
10030        22:11:11:00:00:00    Dynamic                  10.226.14.201,10.226.14.202
Entries in access port
Entries in network port: 3
```

- Show the VXLAN ARP information on Leaf1.

```
admin@Leaf1# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS      VNI       REMOTE-VTEP                 Interface   Status   Age
---------------  -----------------  --------  ----------                  ----------  -------   ------
192.168.0.140    04:f8:f8:20:67:7b  10020                                 ae1          Dynamic  315
172.168.0.200    22:11:11:00:00:00  10030   10.226.14.201,10.226.14.202   vplag-0x2    Dynamic  177
```

- Show the BGP EVPN route information with command **run show bgp evpn route**.

EVPN Multihoming with BUM Tunnel

For the topology and figure in the last section, to enable EVPN multihoming with BUM tunnel, besides above configurations of head end replication, we need to add the following configurations:

- Configure PIM on each device, and configure one of the devices as static RP (Spine2 in this example).
- Configure the same VNI to join the same multicast group.

Leaf1 Configuration

Step 1. Configure PIM and configure Spine2 as static RP.

```
admin@Leaf1# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Leaf1# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Leaf1# set protocols pim interface lo
admin@Leaf1# set protocols pim interface vlan4014
admin@Leaf1# set protocols pim interface vlan4012
```

Step 2. Configure the same VNI to join the same multicast group.

> **NOTE:**
> PICOS supports only one VXLAN segment mapping to one IP multicast group, which is the way to provide the optimal multicast forwarding. That is, to have multiple VXLAN segments share a single IP multicast group in the core network is not supported.

```
admin@Leaf1# set vxlans vni 10020 mcast-group 224.1.1.1
admin@Leaf1# set vxlans vni 10030 mcast-group 230.1.1.1
admin@Leaf1# commit
```

Leaf2 Configuration

```
admin@Leaf2# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Leaf2# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Leaf2# set protocols pim interface lo
admin@Leaf2# set protocols pim interface vlan4014
admin@Leaf2# set protocols pim interface vlan4013
admin@Leaf2# set vxlans vni 10020 mcast-group 224.1.1.1
admin@Leaf2# set vxlans vni 10030 mcast-group 230.1.1.1
admin@Leaf2# commit
```

Leaf3 Configuration

```
admin@Leaf3# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Leaf3# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Leaf3# set protocols pim interface lo
admin@Leaf3# set protocols pim interface vlan4016
admin@Leaf3# set protocols pim interface vlan3012
admin@Leaf3# set vxlans vni 10020 mcast-group 224.1.1.1
admin@Leaf3# set vxlans vni 10030 mcast-group 230.1.1.1
admin@Leaf3# commit
```

Leaf4 Configuration

```
admin@Leaf4# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Leaf4# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Leaf4# set protocols pim interface lo
admin@Leaf4# set protocols pim interface vlan3011
admin@Leaf4# set protocols pim interface vlan3012
```

```
admin@Leaf4# set vxlans vni 10020 mcast-group 224.1.1.1
admin@Leaf4# set vxlans vni 10030 mcast-group 230.1.1.1
admin@Leaf4# commit
```

Spine1 Configuration

```
admin@Spine1# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Spine1# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Spine1# set protocols pim interface lo
admin@Spine1# set protocols pim interface vlan4011
admin@Spine1# set protocols pim interface vlan4092
admin@Spine1# set protocols pim interface vlan4014
admin@Spine1# set protocols pim interface vlan4013
admin@Spine1# set protocols pim interface vlan4015
admin@Spine1# set protocols pim interface vlan4016
admin@Spine1# commit
```

Spine2 Configuration

```
admin@Spine2# set protocols pim rp 202.202.202.202 group 224.1.1.1/32
admin@Spine2# set protocols pim rp 202.202.202.202 group 230.1.1.1/32
admin@Spine2# set protocols pim interface lo
admin@Spine2# set protocols pim interface vlan4011
admin@Spine2# set protocols pim interface vlan4092
admin@Spine2# set protocols pim interface vlan4012
admin@Spine2# set protocols pim interface vlan4014
admin@Spine2# set protocols pim interface vlan4015
admin@Spine2# commit
```

Verify Configuration

In addition to the above show command to verify the results, you can also use the **run show vxlan mcast-tunnel vni** command to view the establishment of the BUM tunnel.

The following example shows the result on Leaf 3:

```
admin@Leaf3# run show vxlan mcast-tunnel vni 10020
VNI       Src-addr         Mcast-addr       Out-Vlan  Out-Interface    Tunnel-ID     Egress-ID
--------  ---------------  ---------------  --------  ---------------  ------------  ------------
10020     10.226.14.201    224.1.1.1        3012      ge-1/1/5         0x4c000000    0

admin@Leaf3# run show vxlan mcast-tunnel vni 10030
VNI       Src-addr         Mcast-addr       Out-Vlan  Out-Interface    Tunnel-ID     Egress-ID
--------  ---------------  ---------------  --------  ---------------  ------------  ------------
10030     10.226.14.201    230.1.1.1        3012      ge-1/1/5         0x4c000001    0
```

EVPN Enhancements

> **Note**
>
> EVPN feature is currently supported on X86 platforms only.

When the switch learns about a local VNI and there is no configuration available in the system regarding this VNI then the import and export route targets (RTs) and route distinguisher (RD) for this VNI will be automatically calculated. The RTs are automatically derived as *AS:VNI,* whereas RD is derived as *Router-ID:VNI-Index.* For Type-2 and Type-3 routes coming from the layer 2 VNI, the RD is calculated as *VXLAN-local0-tunnelip:VNI* instead of *Router-ID:VNI.* Since EVPN routes may have the same MAC and/or the IP address; RDs are used to remove ambiguity in such cases. RTs are used to identify the VPN membership of routes.

For eBGP EVPN peering, since the peers belong to different ASes, using an automatic RT of *AS:VNI* is not suitable for route import. As a result, PICOS uses **:VNI* for the import RT to identify which received routes are relevant to a specific VNI. This behavior occurs only when the switch automatically derives the import RT.

If you do not want that route distinguisher (RD) to be automatically derived, use the command below to manually set the of RD value.

set protocols bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **rd** <*rd*>

If you want route target (RT) to be configured manually instead of being auto-configured, run the command below. The value of parameter route-target can have three values, **export**, **import** or **both**. If you choose **both** then the RT is used as both import and export route target.

set protocols bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **route-target** <*route-target*> **type <both | export | import>**

Example Configuration

Here's an example of how to configure EVPN RD and RT for a specific VNI in a BGP configuration:

1. **Configuring the Route Distinguisher (RD):**

   The Route Distinguisher is used to distinguish between different VPNs in the BGP table. For example, for VNI 100, you can configure RD as `10.10.10.1:100`.

   ```
   set protocols bgp vrf tenant1 evpn vni 100 rd 10.10.10.1:100
   ```

   In this command:
   - `vrf "tenant1"` specifies the VRF instance name.
   - `vni 100` indicates the VNI for which the RD is being configured.
   - `rd 10.10.10.1:100` defines the Route Distinguisher as `10.10.10.1:100`.
2. **Configuring the Route Target (RT):**

   Route Targets control the import and export of routes in a VRF. You can configure the Route Target for a particular VNI using the following command. For example, we will configure an RT with the value `65000:100` and set it for both import and export.

   ```
   set protocols bgp vrf tenant1 evpn vni 100 route-target 65000:100 type both
   ```

   In this command:
   - `vrf "tenant1"` refers to the same VRF.
   - `vni 100` is the same VNI configured earlier.
   - `route-target 65000:100` sets the Route Target value.
   - `type both` specifies that this RT will be used for both import and export. You could also set it for `import` or `export` only, depending on the use case.

Introduction to BGP EVPN

- Introduction
- EVPN Fundamental Configuration
  - Enable EVPN Between BGP Peers
  - Advertise All VNIs Through BGP
    - Note
- EVPN MAC Learning Process
  - Packet Forwarding Process
- ARP/ND Suppression
- Remove EVPN Configuration

NOTEs:

- EVPN feature is currently supported on X86 platforms only.
- To enable a BGP node as a route reflector for EVPN, you need to configure both of the following two commands:

set protocols bgp [vrf <*vrf-name*>**] neighbor** <*bgp-peer*> **route-reflector-client**

set protocols bgp [vrf <*vrf-name*>**] neighbor** <*bgp-peer*> **evpn route-reflector-client**

- The clear command (**run clear mac-address table all** and **run clear arp all**) does not work for manually clearing the dynamic entries in the EVPN MAC address table or ARP address table. These entries can be aged and removed after the Linux kernel aging timer expires.

Introduction

Ethernet Virtual Private Network or EVPN is a technology designed to carry Layer 2 traffic over wide area network protocols. EVPN is a multi-tenant BGP-based control plane for layer-2 (bridging) and layer-3 (routing) VPNs. It's the unifying L2+L3 equivalent of the traditional L3-only MPLS/VPN control plane. PICOS EVPN implementation leverages VXLAN technology as described in RFC7348.

VXLAN has been the predominant technology used in the enterprise and data center domains to achieve Layer 2 level scalability over an IP overlay backbone. VXLAN has become the technology of choice for separating the virtual network from underlying physical network and has greatly enhanced the network virtualization, easier network management and orchestration. VXLANs provides network segmentation but also helps solve the scalability issue normally associated with VLANs.

The following list describes the list of features that PiCOS BGP EVPN implementation supports.

1. Exchange of VNI membership between VTEPs using EVPN type 3 routes.
2. Exchange of host MAC and IP addresses using EVPN type 2 routes.
3. Exchange of MAC Mobility Extended Community to support host/VM mobility.
4. Dual attached host via VXLAN active-active mode. MAC synchronization between switches is achieved via MLAG.
5. Inter Subnet routing for IPv4. Distributed symmetric and asymmetric routing between different subnets and centralized routing.
6. Prefix-based routing using EVPN type-5 routes (EVPN IP prefix route).
7. Multi-tenancy over layer 3.

Both eBGP and iBGP peerings can be used for the EVPN address family.

EVPN Fundamental Configuration

The following steps represent the fundamental configuration to use EVPN as the control plane for VXLAN. These steps are in addition to configuring VXLAN interfaces, attaching them to a bridge, and mapping VLANs to VNIs.

1. Configure Physical interfaces and assign VLANs to interfaces.
2. Configure L3 interfaces and assign IP addresses to interfaces.
3. Configure VXLAN VNIs and enable VXLAN VNI mapping to VLAN IDs.
4. Enable EVPN route exchange (that is, address-family layer 2 VPN/EVPN) between BGP peers.
5. Enable EVPN on the system to advertise VNIs and host reachability information (MAC addresses learned on associated VLANs) to BGP peers.

Additional configuration is necessary such as provision of inter-subnet routing. The configuration depends on the deployment scenario. You can also configure various other BGP parameters depending on your network requirements.

Enable EVPN Between BGP Peers

The very basic steps needed to enable BGP EVPN between a BGP neighbor is as under.

```
admin@router1# set protocols bgp local-as 65101
admin@router1# set protocols bgp router-id 10.10.10.1
admin@router1# set protocols bgp neighbor 100.1.1.134 remote-as 650101
admin@router1# commit
Commit OK.
Save Done!
```

The configuration below adds the evpn address family to the BGP neighbor address-family so that BGP peers activate exchanging EVPN routes with each other. After this configuration, the BGP still does not know about the local VNI's.

Advertise All VNIs Through BGP

To allow BGP know about all VNIs or hosts associated with those local VNIs, enable the BGP control plane for all VNIs using the configuration shown below.

```
admin@router# set protocol bgp evpn advertise-all-vni
admin@router# commit
Commit OK.
Save Done!
```

> **Note**
>
> Only leaf switches that are VTEPs need this configuration. EVPN routes are still accepted from BGP peers as they reside in the global EVPN routing table, but are only made effective when the VNI corresponding to the received route is locally known.

EVPN MAC Learning Process

In **Figure 1**, when Host 1 is first plugged into R1, Host 1 will start sending ARP and other basic networking traffic like DHCP. When R1 receives a packet from Host 1 for the first time, it will record its MAC address in its local MAC address table. Also, R1 will advertise an EVPN Type-2 route to R2. The route includes the local EVPN instance of R1, the VTEP IP address, the Host 1 MAC address and the L2VNI.

Upon receiving the EVPN Type-2 route from R1, R2 learns the MAC address of Host 1. To accept this route, R2 needs to determine if the Import Route Target (IRT) configured on R2 matches the Export Route Target (ERT). RT is sent as the BGP Extended Community

attribute. In this case the IRT and ERT match hence the route is accepted and the MAC address of Host 1 is learned.

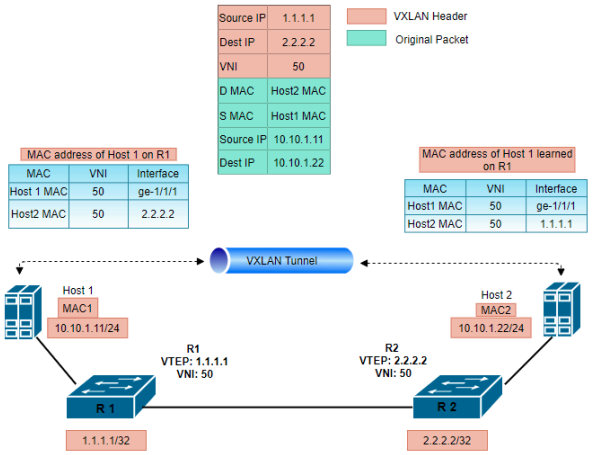


Figure 1. MAC Learning and Packet Forwarding

Packet Forwarding Process

In the case of packet forwarding within the same subnet as depicted in Figure 2, both Host1 and Host2 belong to the same VNI. Host1 wants to send a packet to Host2.

1. If Host1 doesn't have the MAC address of Host1, the MAC address can be learned through the MAC learning process described in the section above. Assuming that Host1 does have the MAC address of Host2, Host 1 sends the packet to R1 destined for Host2.
2. R1 receives the packet and determines the VNI of Host1 based on the ingress interface configuration. R1 learned the Host2 MAC address and the outgoing interface is the VTEP 2.2.2.2 on R2.
3. R1 then encapsulates the original packet from Host1 with the VXLAN header and sends it out.
4. When the packet is received on R2, the outer VXLAN header is stripped off. R2 then searches its local MAC table and finds out the out going interface and delivers the original packet to Host2.

ARP/ND Suppression

Notes:

- ARP/ND suppression does not suppress RA/RS packets.
- When configuring ARP/ND suppression, make sure to configure the L3 VLAN interface corresponding to the VLAN ID associated with the VNI.

In MP-BGP EVPN networks, in order to suppress network storms caused by ARP/ND broadcast message flooding, ARP/ND suppression function can be enabled on VTEP devices to reduce network traffic.

In BGP EVPN networks, VTEPs have the ability to learn both local and remote hosts. When a VTEP learns about a local host from Gratuitous ARP or Reverse ARP, the VTEP will locally record the hosts' MAC and IP address in an ARP Cache Table for that particular VNI. This host MAC and IP address will be shared with remote VTEPs within the same VNI using MP-BGP EVPN Type-2 routes.

When an ARP request broadcast message is received from a host, the local VTEP device with ARP suppression enabled, will actively intercept the message, search the corresponding destination MAC in the VXLAN ARP Cache table, and reply to the ARP message on behalf of the destination host to prevent flooding the entire VXLAN network VNI.

ARP and ND suppression use the same mechanism hence ND suppression is not discussed here.

By default, the ARP/ND suppression function is disabled. Users can use the following command to enable ARP/ND suppression function on VTEP devices.

set vxlans vni <*vni-id*> **arp-nd-suppress disable** <**true** | **false**>

ARP/ND suppression can be enabled on L2 VNI and works only on ARP/ND broadcast messages in the corresponding VNI enabled with this function.

Example configurations:

```
set vlans vlan-id 10
set vxlans vni 10010 vlan 10
set vlans vlan-id 10 l3-interface vlan10
set l3-interface vlan-interface vlan10
set vxlans vni 10010 arp-nd-suppress disable false
```

Remove EVPN Configuration

Warning:

To correctly remove EVPN configuration, the following deletion sequence needs to be followed.

1. First, remove the data plane configuration, that is, VXLAN-related configuration, including commands under the following configuration node: **set vxlans** xxx.
2. Then, remove the control plane configuration, that is, BGP and BGP EVPN related configurations, including commands under the following configuration node: **set protocols bgp** xxx.
3. Last, delete VXLAN related L3 interface configuration, including the following commands:

   set l3-interface vlan-interface xxx

   set l3-interface routed-interface xxx

If you don't follow this deletion order, the configuration in the kernel may still exist after the deletion operation, inconsistency in two systems (PICOS and kernel) may lead to unpredictable problems.

Generic Routing Encapsulation Protocol (GRE)

- Overview
- GRE Configuration Example

Overview

NOTE:

- GRE is not supported on Dell N22xx series switches and N3208PX-ON switch.
- PicOS GRE supports tunneling of IPv4 over IPv4 and IPv6 over IPv4.
- One GRE tunnel source address and destination address form an address pair. Different GRE tunnels cannot be configured with the same address pair.
- In the same VRF, it is not allowed to configure different GRE tunnel interface addresses with the same network segment IP address.
- If a large number of static routes for the GRE tunnel are configured and committed at one time, the background process will take several minutes to successfully complete all these configurations, although the print may immediately show that the commit is OK.
- On AS4610 serial switches, the number of static routes for the GRE tunnel should be not more than 20.
- By default, the MTU value of an L3 interface is 1500. If you want to change the MTU value of the GRE tunnel source interface, its value should be less than 1304.

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate almost any network layer protocol and delivers it over an IP network. GRE is defined by two tunnel endpoints, the GRE source and destination endpoint. From the common user perspective the two endpoints appear as if they are directly connected in a point-to-point configuration but in reality the packet may traverse a number of hops before it reaches the destination endpoint. The generic packet format of a GRE encapsulated packet is show in Figure 1.

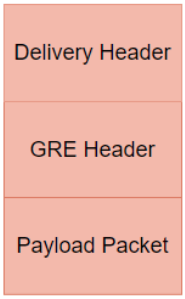
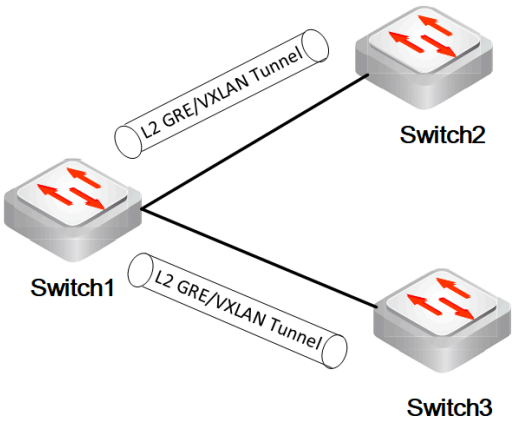


Figure 1. GRE Packet Format

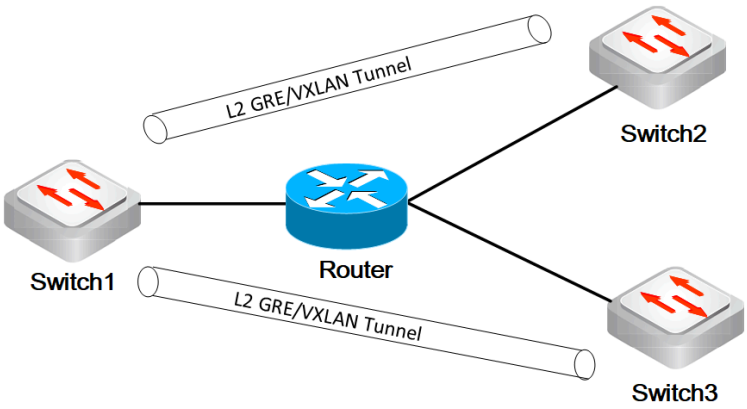
The original payload packet is first encapsulated with the GRE header and then encapsulated again with the delivery protocol header to transport it over the network. For example, if the network doesn't support routing IPv6 packets, the packet can be encapsulated with GRE header and then use IPv4 as the delivery protocol to transport the packet. The packet is decapsulated at the destination endpoint and the actual IPv6 packet is forwarded to the destination. One of the most common issue in enterprise networks is that on local subnets private IP addresses are used but routing packets between different subnets via private IP headers is not supported over public networks such as the internet. This issue is solved by using GRE which can encapsulate packets into a delivery protocol header that can be transported over the public network.

Application Scenario Limitation

In L2 GRE or VXLAN networks, only one next hop is allowed for the same egress interface. In the following figure, the same egress interface on Switch1 has two tunnels, that is, two next hops, which is not allowed.



However, multiple L2 GRE or VXLAN tunnels can exist from the same egress port on Switch1 if connected via the IP router, ensuring that one egress interface has only one next hop, as shown in the figure below.


L2 GRE/VXLAN Tunnel
Switch2
Switch1
Router
L2 GRE/VXLAN Tunnel
Switch3

GRE Configuration Example

NOTE:
GRE tunnel is a logical interface created by Linux kernel on software side. Once created, GRE tunnel stays in "**UP**" state unless it is shut down by CLI command "**set l3-interface tunnel xxx disable**".

For example, as shown in **Figure 1**, if physical port ge-1/1/1 is down, the underlay routing of the associate GRE tunnel is broken. It is not necessary that tunnel interface (tnl0) should be down. In this case, the state of GRE tunnel is "UP" in the display of show command **run show l3-interface tunnel**.

```
admin@R1# run show l3-interface tunnel tnl0
tnl0        State:UP
            Tunnel Source: 100.168.3.1
            Tunnel Destnation:: 100.168.10.2
            Tunnel protocol/transport: gre-ip
            Inet addr: 100.168.4.1
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.............................28
              IPv4 Forwarding Packets.......................5
              IPv6 Input Packets.............................0
              IPv6 Forwarding Packets.........
```

In this document we will demonstrate a sample use case for GRE tunnels using two PICOS switches. As shown in Figure 1, we have two Pica8 switches connected to each other through a public IPv4 network. A host is connected with each device.

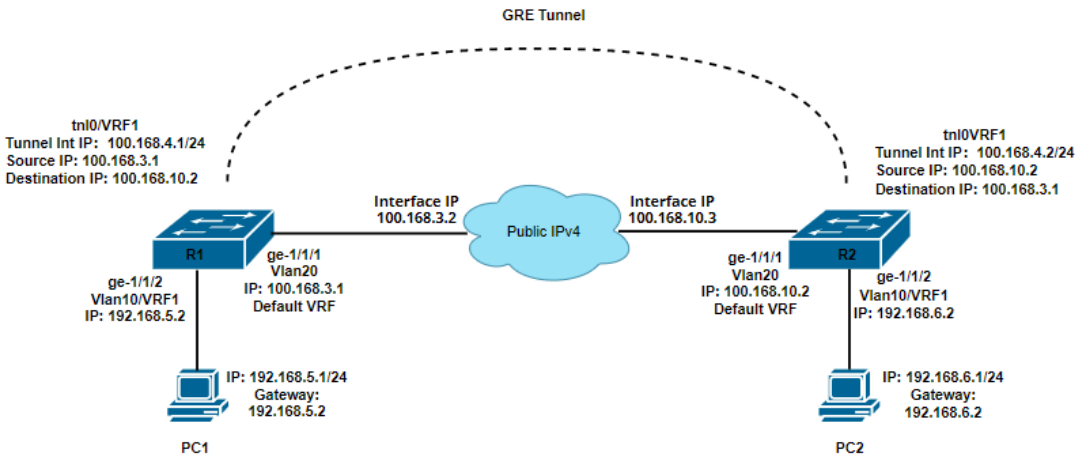


Figure 1. GRE Tunnel Configuration

Switch configurations

Below is the switch R1 and R2 configurations.

R1 Configuration

Step 1: Configure L3 VLAN interface for GRE tunnel.

```
admin@R1# set vlans vlan-id 20 l3-interface "vlan20"
admin@R1# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@R1# set l3-interface vlan-interface vlan20 address 100.168.3.1 prefix-length 24
```

Step 2: Configure L3 VLAN interface for PC1.

```
admin@R1# set vlans vlan-id 10 l3-interface "vlan10"
```

```
admin@R1# set l3-interface vlan-interface vlan10 vrf "vrf1"
admin@R1# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@R1# set l3-interface vlan-interface vlan10 address 192.168.5.2 prefix-length 24
```

Step 3: Enable IP routing on R1 and configure VRF.

```
admin@R1# set ip routing enable true
admin@R1# set ip vrf vrf1 description "orange"
```

Step 4. Configure GRE tunnel name, IP, source IP, destination IP etc.

```
admin@R1# set l3-interface tunnel tnl0 address 100.168.4.1 prefix-length 24
admin@R1# set l3-interface tunnel tnl0 tunnel-mode "gre-ip"
admin@R1# set l3-interface tunnel tnl0 source 100.168.3.1
admin@R1# set l3-interface tunnel tnl0 destination 100.168.10.2
admin@R1# set l3-interface tunnel tnl0 vrf "vrf1"
```

Step 5: Create static routes for the GRE tunnel.

```
admin@R1# set protocols static vrf vrf1 route 192.168.6.0/24 next-hop 100.168.4.2
admin@R1# set protocols static route 100.168.10.0/24 next-hop 100.168.3.2
```

Or we can create the static route using the tunnel name as the next hop.

```
admin@R1# set protocols static vrf vrf1 interface-route 192.168.6.0/24 interface tnl0
```

R2 Configuration

Step1. Configure L3 VLAN interface for GRE tunnel.

```
admin@R2# set vlans vlan-id 20 l3-interface "vlan20"
admin@R2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 20
admin@R2# set l3-interface vlan-interface vlan20 address 100.168.10.2 prefix-length 24
```

Step 2: Configure L3 VLAN interface for PC2.

```
admin@R2# set vlans vlan-id 10 l3-interface "vlan10"
admin@R2# set l3-interface vlan-interface vlan10 vrf "vrf1"
admin@R2# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@R2# set l3-interface vlan-interface vlan10 address 192.168.6.2 prefix-length 24
```

Step 3: Enable IP routing on R1 and configure VRF.

```
admin@R2# set ip routing enable true
admin@R2# set ip vrf vrf1 description "orange"
```

Step 4. Configure GRE tunnel name, IP, source IP, destination IP etc.

```
admin@R2# set l3-interface tunnel tnl0 address 100.168.4.2 prefix-length 24
admin@R2# set l3-interface tunnel tnl0 tunnel-mode "gre-ip"
admin@R2# set l3-interface tunnel tnl0 source 100.168.10.2
admin@R2# set l3-interface tunnel tnl0 destination 100.168.3.1
admin@R2# set l3-interface tunnel tnl0 vrf "vrf1"
```

Step 5: Create static routes for the GRE tunnel.

```
admin@R2# set protocols static vrf vrf1 route 192.168.5.0/24 next-hop 100.168.4.1
admin@R2# set protocols static route 100.168.3.0/24 next-hop 100.168.10.3
```

Or we can also create the static route with the tunnel name as the next hop.

```
admin@R2# set protocols static vrf vrf1 interface-route 192.168.5.0/24 interface tnl0
```

Verify Configuration

- Run command **run show l3-interface tunnel** to display information about the GRE tunnel interface.

```
admin@R1# run show l3-interface tunnel tnl0
tnl0        State:UP
            Tunnel Source: 100.168.3.1
            Tunnel Destnation:: 100.168.10.2
            Tunnel protocol/transport: gre-ip
            Inet addr: 100.168.4.1
            Traffic statistics:
              5 sec input rate IPv4 1400 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 28 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................28
              IPv4 Forwarding Packets....................5
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
```

- To verify the configuration on R1, we can use the command **show l3-interface tunnel tnl0** as shown below.

```
admin@R1# show l3-interface tunnel tnl0
    address 100.168.4.1 {
        prefix-length: 24
    }
    tunnel-mode: "gre-ip"
    source: 100.168.3.1
    destination: 100.168.10.2
    vrf: "vrf1"
```

- Similarly on R2, run the same command.

```
admin@R2# show l3-interface tunnel tnl0
    address 100.168.4.2 {
        prefix-length: 24
    }
    tunnel-mode: "gre-ip"
    source: 100.168.10.2
    destination: 100.168.3.1
    vrf: "vrf1"
```

- Check to see if PC1 can reach PC2.

```
PC1# ping 192.168.6.1
PING 192.168.6.1 (192.168.6.1) 56(84) bytes of data.
64 bytes from 192.168.6.1: icmp_seq=1 ttl=64 time=3.064 ms
64 bytes from 192.168.6.1: icmp_seq=2 ttl=64 time=2.062 ms
64 bytes from 192.168.6.1: icmp_seq=3 ttl=64 time=1.060 ms
```

MPLS Configuration

- MPLS Overview
- Configuration Restrictions and Guidlines
- Basic MPLS LDP Configuration
- (Optional) Configuring MPLS LDP Security
- (Optional) Configuring MPLS LDP Timers
- (Optional) Configuring MPLS LDP to Allocate Labels for Host Routes Only
- (Optional) Configuring MPLS LDP PHP (Penultimate Hop Popping)
- Example for Configuring MPLS LDP
- RFC Lists for MPLS

MPLS Overview

- What is MPLS ?
- MPLS Label Distribution Protocol
  - Core Components and Processes
  - Major LDP Message Types
- Use Cases

What is MPLS ?

Multiprotocol Label Switching (MPLS) is a network transmission technology used to efficiently forward data packets from source to destination. Unlike traditional IP routing, MPLS does not route based on destination addresses but rather on short labels attached to packets, enabling faster and more efficient data forwarding.

MPLS works by attaching short labels to data packets and using these labels to guide the packets through a network. Here's how MPLS works on PICOS switches in more detail:

1. **Label Assignment**: When a packet enters an MPLS network, the ingress router assigns a label to the packet. This label is a short identifier that represents a particular path or route through the network.
2. **Label Switching**: As the labeled packet travels through the MPLS network, each router along the path uses the label to make forwarding decisions. Instead of examining the packet's IP header to determine the next hop, routers only need to look at the label, which makes forwarding decisions much faster and more efficient.
3. **Label Distribution**: MPLS routers use protocols like LDP (Label Distribution Protocol) or RSVP-TE (Resource Reservation Protocol - Traffic Engineering) to exchange label information and establish Label Switched Paths (LSPs) through the network. This ensures that all routers in the network have the necessary label mappings to forward packets correctly.

MPLS Label Distribution Protocol

The Label Distribution Protocol (LDP) is a key protocol within the MPLS framework that is responsible for the distribution and management of labels used in MPLS networks. LDP enables MPLS to establish LSPs, which guide the forwarding of data packets through the network based on these labels.

Core Components and Processes

1. Discovery

- **Discovery Process**: LDP utilizes UDP to discover neighboring LSRs by sending Hello messages.
- **Neighbor Identification**: These Hello messages help LSRs in identifying and validating neighboring routers in the network.

2. Session Establishment

- **TCP Session**: Once neighbors are discovered, LSRs establish a TCP connection to create a control session.
- **Session Initialization**: LDP Initialization messages are exchanged to negotiate protocol parameters, confirming that both LSRs can communicate.

3. Label Distribution

- **Label Binding**: LSRs distribute label bindings via LDP messages. When an LSR receives an IP prefix for a specific destination, it creates a label for that prefix.
- **Message Types**: Key LDP messages include Label Mapping (to distribute the label bindings) and Label Request (to ask for label binding information from peers).

4. **Path Maintenance**

- **Monitoring**: LDP continually monitors the network and updates label bindings as network conditions change.
- **Fault Management**: Notification messages are used to report errors and to help diagnose problems, ensuring the robustness of LSPs.

Major LDP Message Types

LDP itself utilizes a number of message types for its operations. Here are the major LDP message types:

- **Discovery (Hello) Messages**: Facilitate the discovery of neighboring LSRs.
- **Session Establishment Messages**: Manage the establishment and maintenance of LDP sessions, including Initialization and Keepalive messages.
- **Advertisement Messages**: Distribute label bindings using Label Mapping, Label Request, and other advertisement messages.

These LDP messages work together to establish and maintain LSPs that facilitate efficient packet forwarding in an MPLS network. Each type of message plays a specific role in label distribution, session management, and error handling.

Use Cases

MPLS is widely used in various applications across different industries due to its flexibility, efficiency, and reliability. Here are some common use cases of MPLS:

- **Service Provider Networks**

  Service providers use MPLS to offer Layer 3 Virtual Private Networks (VPNs) and Layer 2 VPNs (VPLS), providing private, isolated networks over a shared infrastructure.

  MPLS is used to efficiently route multiple types of internet traffic, including business-critical applications, over the same backbone.

- **Enterprise Networks**

  MPLS is frequently used by enterprises to connect branch offices, data centers, and headquarters over a private WAN, providing secure, reliable, and efficient communication.

  MPLS ensures low latency and high reliability for voice and video traffic, making it ideal for VoIP and unified communications applications.

- **Data Center Interconnection**

  LDP optimizes the flow of data between data centers, enhancing connectivity and performance.

Configuration Restrictions and Guidlines

When you configure MPLS, follow these restrictions and guidelines:

- MPLS is supported only on **Trident3-X7** platforms, which include the following switches: N8550-48B8C, N8550-32C, N8560-32C, S5232F-ON, S5248F-ON and S5296F-ON.
- Currently, PICOS supports only MPLS LDP; static MPLS is not supported.
- MPLS does not support ECMP (Equal-Cost Multi-Path) routing.

  Ensure that ECMP configurations are not applied to MPLS-enabled interfaces or paths to avoid any unexpected behavior or network issues.
- LDP can only be configured in the default VRF (Virtual Routing and Forwarding instance). This means that if all router interfaces are moved to a user-defined VRF, the functionality of LDP may be affected because LDP cannot run in these user-defined VRFs, which could result in the failure of LSPs (Label Switched Paths).

Basic MPLS LDP Configuration

- Enable MPLS on Interfaces
- Configuring a Router ID
- Enable MPLS LDP on the L3 Interface
- Configure MPLS LDP Transport Address
- (Optional) Enable Ordered Control Mode for MPLS LDP
  - Advantages When Using Ordered-Control
  - Example
- Verify LDP Neighbor Discovery

> **NOTE:**
>
> Before configuring MPLS, routing protocols such as OSPF/ ISIS need to be configured on each LSR to achieve IP connectivity between LSRs.

MPLS (Multiprotocol Label Switching) is a technique used in modern networking to improve packet forwarding efficiency by using labels rather than traditional IP routing. **Label Distribution Protocol (LDP)** is the most commonly used protocol for distributing labels in MPLS networks. It is responsible for establishing and maintaining Label-Switched Paths (LSPs) by advertising the mapping between IP prefixes and labels across routers.

This section provides a comprehensive description of basic MPLS LDP configuration and its importance in a typical MPLS network.

Enable MPLS on Interfaces

Before enabling LDP, MPLS must be enabled on each interface that will participate in the MPLS label switching process.

- The following example enables MPLS on VLAN interface *vlan200*.

```
admin@PICOS# set protocols mpls interface vlan200
admin@PICOS# commit
```

This ensures that MPLS forwarding is active on the specified L3 interface (VLAN interface, loopback interface, routed interface or sub-interface). This enables MPLS for all traffic passing through that interface, making it part of the MPLS domain for the labeled packet switching. Usually, both the incoming and outgoing interfaces of the packets need to enable MPLS.

Configuring a Router ID

The router ID should be configured first when you configure MPLS LDP. The router ID is a string similar to the IP address, and is the identifier of a LSR. You should not change the router ID after completing the configuration. By default, the MPLS LDP router ID is not configured.

```
admin@PICOS# set protocols mpls ldp router-id 2.2.2.2
admin@PICOS# commit
```

Enable MPLS LDP on the L3 Interface

LDP must be explicitly enabled on each interface that will be used for label distribution. This ensures that LDP neighbors are discovered on those interfaces and that labels are exchanged.

The following command can be used to enable MPLS LDP on an L3 interface under IPv4/IPv6 address family.

set protocols mpls ldp {ipv4-family|ipv6-family} interface *<interface-name>*

It is required to be configured on all nodes in the MPLS domain.

MPLS can support multiple protocol families (IPv4, IPv6, etc.). By specifying `ipv4-family (ipv6-family)`, you ensure that LDP only distributes labels for IPv4 (IPv6) prefixes over this interface.

- The following commands enable MPLS LDP on interface vlan200 of IPv4 address family.

```
admin@PICOS# set protocols mpls ldp ipv4-family interface vlan200
admin@PICOS# commit
```

- The following commands enable MPLS LDP on interface vlan400 of IPv6 address family.

```
admin@PICOS# set protocols mpls ldp ipv6-family interface vlan400
admin@PICOS# commit
```

Once LDP is enabled on the L3 interface for the IP family, the router starts advertising and learning labels for IP routes over this interface.

Configure MPLS LDP Transport Address

This address is used as the source address in the Hello message of LDP link.
LDP session is based on TCP connection, when two LSRs want to establish an LDP session between them, they need to confirm the LDP transport address of the peer before they can establish a TCP connection.

- The following commands configure MPLS LDP transmission address under IPv4 address family.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery transport-address 2.2.2.2
admin@PICOS# commit
```

- The following commands configure MPLS LDP transmission address under IPv6 address family.

```
admin@PICOS# set protocols mpls ldp ipv6-family discovery transport-address 1::1
admin@PICOS# commit
```

(Optional) Enable Ordered Control Mode for MPLS LDP

In MPLS LDP, ordered control is one of two label distribution modes (the other being independent control). In **ordered control**, a router only distributes a label for a particular FEC (Forwarding Equivalence Class) if it is the egress router for that FEC, or if it has already received a label for that FEC from its next hop. This ensures a more structured and synchronized label distribution process.

Independent Control (the alternative mode) allows routers to advertise labels for a FEC as soon as they learn about it, without waiting for downstream routers to assign labels. This the default label distribution mode for MPLS LDP.

Advantages When Using Ordered-Control

Enabling ordered control offers the following advantages; therefore, it is recommended to enable the ordered control mode.

- Label distribution is more controlled and happens from downstream routers to upstream routers.
- It helps to avoid issues such as forwarding loops in complex network topologies.
- Useful in situations where label distribution must be tightly synchronized between routers.

Example

- Enable LDP Ordered Label Distribution Control.

```
admin@PICOS# set protocols mpls ldp ordered-control
admin@PICOS# commit
```

This command would typically be configured on MPLS-enabled routers to ensure they follow the ordered control mode for LDP, improving synchronization and reducing potential issues with label assignment.

Verify LDP Neighbor Discovery

- After configuration, check that LDP neighbors are discovered. Run the command **run show mpls ldp neighbor** to display the current LDP neighbors.
- Ensure that the router has assigned labels to IP routes and that the labels are being advertised to LDP neighbors. You can use the command **run show mpls ldp binding** to view Label Information Base (LIB) information.

(Optional) Configuring MPLS LDP Security

Enable MD5 Authentication between MPLS LDP Neighbors
Enable Generalized TTL Security Mechanism (GTSM)

In networks where security requirements are high, network security can be enhanced by configuring LDP MD5 authentication and LDP GTSM.

Enable MD5 Authentication between MPLS LDP Neighbors

In order to enhance the security of LDP session connections, MD5 authentication can be configured for the TCP connections used by LDP.

By setting a password, you enforce authentication for the LDP session between the local router and its neighbor. This adds a layer of security, ensuring that only authorized routers can establish an LDP session and exchange label information.

It helps to prevent unauthorized devices from establishing LDP sessions with your routers, which could potentially lead to routing issues or security vulnerabilities.

NOTE:

Ensure that the same password is configured on both sides of the LDP session. Mismatched passwords will prevent the LDP session from being established.

This example enables message digest5 (MD5) authentication on a TCP connection between two MPLS LDP neighbors.

```
admin@XorPlus# set protocols mpls ldp neighbor 2.2.2.2 password picos12345
admin@XorPlus# commit
```

Enable Generalized TTL Security Mechanism (GTSM)

The Generalized TTL Security Mechanism (GTSM) is a security mechanism used to protect devices from attacks by determining the validity of packets based on their TTL (Time-to-Live) values. When configured on LDP peers, GTSM checks the TTL values of LDP messages exchanged between peers based on the configured TTL range. If the TTL of an LDP message does not fall within the configured range, it is considered an illegal attack packet and is discarded. This helps prevent attacks on the LDP protocol that involve flooding the network with forged packets, thereby protecting the upper-layer protocols.

The **set protocols mpls ldp neighbor ttl-security hops** command enforces Generalized TTL Security Mechanism (GTSM), as specified in RFC 5082. With this command, only neighbors that are the specified number of hops away will be allowed to become neighbors. This command is mutually exclusive with ebgp-multihop.

By default, TTL hop is 0, indicating **ttl-security** is disabled.

NOTE:

- The valid range of TTL values allowed for detection packets varies among devices from different vendors, including 1 to 255 and 1 to 64. Therefore, when interoperating with devices from other vendors, it is necessary to configure different hop values according to the implementation of the other vendor's devices. Otherwise, packets sent by the peer will be discarded, leading to interruption of the LDP session.
- The commands **set protocols mpls ldp neighbor** <*ip*> **ttl-security hops** <*integer*> and **set protocols mpls ldp neighbor** <*ip*> **ttl-security disable** cannot be configured simultaneously.

This following example enables GTSM and configures GTSM valid hops.

```
admin@PICOS# set protocols mpls ldp neighbor 2.2.2.2 ttl-security hops 10
admin@PICOS# commit
```

Disabling GTSM might be necessary if compatibility with older or certain specific devices that do not support TTL security is required. The following command can be used to disable GTSM.

```
admin@PICOS# set protocols mpls ldp neighbor 2.2.2.2 ttl-security disable
admin@PICOS# commit
```

(Optional) Configuring MPLS LDP Timers

Configure the Link Hello Sending Timer
Configure the Link Hello Hold Time
Configure the Hold Time Period for Keepalive
Configure the Interval for Sending Targeted Hello Messages
Configure the Targeted Hello Hold Time

LDP uses the discovery process to identify other LDP-enabled routers in the network. The discovery process involves sending "Hello" messages, which can be of two types:

- **Link Hello**: These are sent to directly connected neighbors over a specific interface.
- **Targeted Hello**: These are sent to establish sessions with non-directly connected peers.

Configure the Link Hello Sending Timer

NOTEs：

- Before configuring the **discovery hello-interval** and **discovery hello-holdtime**, the **discovery transport-address** under the IP family must be configured first.
- The configuration of **discovery hello-interval** and **discovery hello-holdtime** based on the IP family takes precedence over the global configuration.
- For the **discovery hello-interval (discovery hello-holdtime)** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

The LSR uses the Hello interval to periodically send Hello messages, notifying neighboring LSRs of its presence in the network and establishing Hello adjacency relationships. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 5 seconds.

- Configure the interval for sending Hello message.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery hello-interval 10
admin@PICOS# commit
```

Configure the Link Hello Hold Time

LDP peers that have established a Hello adjacency relationship periodically send Hello messages to signify their intention to maintain this adjacency. If no new Hello message is received before the Hello hold timer expires, the adjacency will be terminated. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 15 seconds. It is recommended to use the default value.

- Configure the Hello hold time.

```
admin@PICOS# set protocols mpls ldp ipv6-family discovery hello-holdtime 30
admin@PICOS# commit
```

- Show the configuration result.

```
admin@PICOS# run show mpls ldp interface
AF   Interface   State  Uptime   Hello Timers  ac
ipv6 vlan10      ACTIVE 3d18h21m 5/30           1
```

```
ipv6 vlan20      ACTIVE 3d18h21m 5/30          1
ipv6 vlan30      ACTIVE 01:02:58 5/30          1
ipv6 vlan40      ACTIVE 00:48:21 5/30          0
```

Configure the Hold Time Period for Keepalive

Between LDP peers, LDP sessions are maintained through LDP protocol messages (PDUs). If the Keepalive hold timer expires without receiving any LDP PDUs, the connection is closed, and the LDP session ends. That value is an integer which can be configured between 15 and 65535 seconds. By default, LDP session holdtime 180 seconds.

The Keepalive sent interval is the time for the LSR to periodically send Hello messages, and it is 1/3 of the Keepalive hold timer.

- Configure the hold time period for keepalive.

```
admin@PICOS# set protocols mpls ldp neighbor 3.3.3.3 session-holdtime 210
admin@PICOS# commit
```

- Show the configuration result.

```
admin@PICOS# run show mpls ldp neighbor detail
Peer LDP Identifier: 3.3.3.3:0
  TCP connection: 2::2:646 - 3::3:34795
  Authentication: none
  Session Holdtime: 210 secs; KeepAlive interval: 70 secs
  State: OPERATIONAL; Downstream-Unsolicited
  Up time: 2d19h07m
  Messages sent/rcvd:
   - Keepalive Messages: 4022/4024
   - Address Messages: 1/3
   - Address Withdraw Messages: 3/3
   - Notification Messages: 0/0
   - Capability Messages: 0/0
   - Label Mapping Messages: 128/70
   - Label Request Messages: 0/0
   - Label Withdraw Messages: 16/10
   - Label Release Messages: 10/16
   - Label Abort Request Messages: 0/0
  Capabilities Sent:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  Capabilities Received:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  LDP Discovery Sources:
    IPv6:
      Interface: vlan30
```

Configure the Interval for Sending Targeted Hello Messages

NOTEs：

- Before configuring the **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime**, the **targeted-hello-accept** under the IP family must be enabled first.
- The configuration of **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime** based on the IP family takes precedence over the global configuration.

- For the **targeted-hello-holdtime (discovery targeted-hello-interval)** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Users can set the interval (in seconds) at which the targeted Hello messages are sent out to maintain LDP sessions with non-directly connected peers. A shorter interval means more frequent Hellos, which can help in quicker detection of peers but may increase the load on the router.

The value is an integer which can be configured between 1 and 65535 seconds. The default value is 5 seconds.

- Configure the interval for sending targeted hello messages.

```
admin@PICOS# set protocols mpls ldp discovery targeted-hello-interval 10
admin@PICOS# commit
```

Configure the Targeted Hello Hold Time

The `targeted-hello-holdtime` parameter sets the amount of time (in seconds) that the router will wait after receiving the last Hello message before considering the neighbor as unreachable. If the router does not receive another Hello message from the neighbor within this period, it will consider the neighbor to be down and will tear down the LDP session associated with that neighbor.

This timer ensures that the LDP session is maintained as long as the neighbor is responsive. It is a fail-safe mechanism that helps in quickly detecting and reacting to network changes.

The value is an integer which can be configured between 1 and 65535 seconds. The default value is 15 seconds.

Administrators can adjust this value to either lengthen or shorten the period before the router considers the neighbor unreachable. A shorter hold time means the router will more quickly declare the neighbor down if no Hello messages are received, while a longer hold time will delay this declaration, potentially allowing more time for transient issues to resolve.

- Configure the targeted hello hold time.

```
admin@PICOS# set protocols mpls ldp discovery targeted-hello-holdtime 50
admin@PICOS# commit
```

(Optional) Configuring MPLS LDP to Allocate Labels for Host Routes Only

LDP can allocate labels for various types of routes in the routing table. These routes can include network prefixes, host routes (which are more specific and typically represent individual IP addresses), and other types of routes.

A host route is a route to a specific IP address with a /32 (in IPv4) or /128 (in IPv6) prefix length. This means that the route is specific to one single host or device on the network, rather than a range of IP addresses.

The **set protocols mpls ldp {ipv4-family|ipv6-family} label-local-allocate host-routes** command instructs the router to allocate MPLS labels specifically for host routes in the IPv4/IPv6 routing table. Without this command, LDP may only allocate labels for network routes (e.g., /24, /40) and not for individual host routes (/32 and /128).

Use Cases

- **Data Centers**: In data center networks where traffic to specific servers or services must be carefully managed, allocating labels to host routes allows for precise traffic engineering.
- **Service Provider Networks**: In service provider networks where certain customers require dedicated paths to their services, host route label allocation can ensure that traffic is routed optimally.
- **Security Considerations**: Allocating labels for host routes can be part of a security strategy where certain traffic is routed through specific security appliances or paths.

Example

- The following command configures the router to allocate MPLS labels for all host routes in the IPv4 routing table. As a result, any route in the routing table with a /32 prefix length will be associated with an MPLS label, allowing for the forwarding of traffic destined for that specific IP address using MPLS.

```
admin@PICOS# set protocols mpls ldp ipv4-family label-local-allocate host-routes
admin@PICOS# commit
```

(Optional) Configuring MPLS LDP PHP (Penultimate Hop Popping)

Penultimate Hop Popping (PHP) is a fundamental concept in MPLS networks. It refers to the process where the second-to-last router (penultimate hop) in a Label Switched Path (LSP) removes (or "pops") the MPLS label from a packet before forwarding it to the last router (the egress router). This technique helps optimize network performance and reduce processing overhead on the egress router.

Purpose and Benefits of PHP

- **Reduced Processing Load**: PHP offloads the task of MPLS label removal from the egress router, reducing its processing burden. This is particularly beneficial in high-throughput environments where the egress router may be handling large amounts of traffic.
- **Simplified Egress Processing**: The egress router receives the packet as a regular IP packet, which simplifies its processing because it no longer needs to look up and remove an MPLS label before making a forwarding decision.
- **Efficiency**: PHP reduces the overhead of MPLS label operations at the final hop, which can improve overall network efficiency.

How PHP Works

In a typical MPLS scenario, each router along the LSP swaps the incoming MPLS label with a new label before forwarding the packet to the next hop. However, when the packet reaches the penultimate hop, instead of swapping the label, the router pops the label (removes it entirely).

The packet is then forwarded as a regular IP packet (or with an explicit null label if that is configured) to the egress router.

PHP and Implicit Null Label

- The mechanism behind PHP is often tied to the use of the **Implicit Null Label** (label value 3). When an MPLS router advertises the implicit null label to its upstream neighbor, it instructs the penultimate hop to pop the MPLS label and forward the packet as a plain IP packet.
- **Implicit Null Label**: This label is not actually carried in the packet. Instead, it tells the penultimate router to remove the label and forward the packet without any MPLS label.

Explicit Null as an Alternative to PHP

Instead of using PHP, an explicit null label (label value 0 for IPv4) can be used. With explicit null, the MPLS label is preserved (though replaced with the explicit null label), allowing the egress router to receive and process the QoS (Quality of Service) information that might be encoded in the MPLS header.

Configuration

The **set protocols mpls ldp {ipv4-family|ipv6-family} label-local-advertise [explicit-null]** command configures the label assigned for the penultimate router under the address family on the egress LSP. The **explicit-null** option assigns an explicit null label(0), to the penultimate router. If **explicit-null** option is not specified, or this command is not configured, the LSR assigns an implicit null label(3), to the penultimate router.

Example

- The following command configures to assign an explicit null label for the penultimate router on the egress LSP.

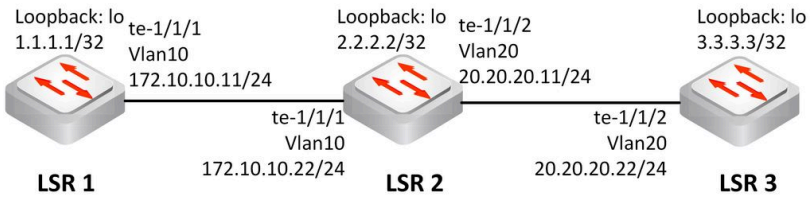
```
admin@PICOS# set protocols mpls ldp ipv4-family label-local-advertise explicit-null
admin@PICOS# commit
```

Example for Configuring MPLS LDP

Network Requirement
Procedure
LSR 1
LSR 2
LSR 3
Verify the Configuration

Network Requirement

Figure 1. MPLS LDP Configuration Example



LSR 1 and LSR 3 serve as the PE (Provider Edge) devices in the IP/MPLS backbone network. MPLS LDP (Label Distribution Protocol) needs to be configured on both LSR 1 and LSR 3 to establish LDP LSPs (Label Switched Paths), enabling the interconnection of LSP networks and supporting business traffic transmission.

Configure MPLS LDP as follows:

1. Configure OSPF on each LSR to ensure IP connectivity in the backbone network. This includes configuring OSPF protocol and relevant network segments, areas, and neighbor relationships.
2. Configure MPLS LDP on each LSR. This involves enabling MPLS functionality and configuring LDP protocol parameters such as LDP session parameters, LDP neighbor relationships, and LDP label distribution policies.

With this configuration, each LSR will be able to establish an IP/MPLS network and create LDP LSPs through MPLS LDP, thereby achieving interconnection and business transmission of LSP networks.

Procedure

LSR 1

Step 1 Configure VLAN interface.

```
admin@LSR1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@LSR1# set l3-interface vlan-interface vlan10 address 172.10.10.11 prefix-length 24
admin@LSR1# set vlans vlan-id 10 l3-interface vlan10
admin@LSR1# set l3-interface loopback lo1 address 1.1.1.1 prefix-length 32
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node's interfaces and the LSR's host routes.

```
admin@LSR1# set protocols ospf router-id 1.1.1.1
admin@LSR1# set protocols ospf network 172.10.10.0/24 area 0
```

```
admin@LSR1# set protocols ospf network 1.1.1.1/32 area 0
```

Step 3 Enable MPLS on the L3 interface.

```
admin@LSR1# set protocols mpls interface vlan10
```

Step 4 Enable MPLS LDP on the L3 interface.

```
admin@LSR1# set protocols mpls ldp ipv4-family interface vlan10
```

Step 5 Configure MPLS router ID.

```
admin@LSR1# set protocols mpls ldp router-id 1.1.1.1
```

Step 6 Configure MPLS LDP transmission address under IPv4 address family.

```
admin@LSR1# set protocols mpls ldp ipv4-family discovery transport-address 1.1.1.1
```

Step 7 Configure LDP ordered label distribution control.

```
admin@LSR1# set protocols mpls ldp ordered-control
```

Step 8 Enable IP routing.

```
admin@LSR1# set ip routing enable true
```

Step 9 Commit the configuration.

```
admin@LSR1# commit
```

LSR 2

Step 1 Configure VLAN interface.

```
admin@LSR2# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
admin@LSR2# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@LSR2# set l3-interface vlan-interface vlan10 address 172.10.10.22 prefix-length 24
admin@LSR2# set l3-interface vlan-interface vlan20 address 20.20.20.11 prefix-length 24
admin@LSR2# set vlans vlan-id 10 l3-interface vlan10
admin@LSR2# set vlans vlan-id 20 l3-interface vlan20
admin@LSR2# set l3-interface loopback lo2 address 2.2.2.2 prefix-length 32
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node's interfaces and the LSR's host routes.

```
admin@LSR2# set protocols ospf router-id 2.2.2.2
admin@LSR2# set protocols ospf network 172.10.10.0/24 area 0
admin@LSR2# set protocols ospf network 20.20.20.0/24 area 0
admin@LSR2# set protocols ospf network 2.2.2.2/24 area 0
```

Step 3 Enable MPLS on the L3 interface.

```
admin@LSR2# set protocols mpls interface vlan10
admin@LSR2# set protocols mpls interface vlan20
```

Step 4 Enable MPLS LDP on the L3 interface. Usually, both the incoming and outgoing interfaces of the packets need to enable MPLS. By default, MPLS is disabled on the L3 interface.

```
admin@LSR2# set protocols mpls ldp ipv4-family interface vlan10
```

```
admin@LSR2# set protocols mpls ldp ipv4-family interface vlan20
```

Step 5 Configure MPLS router ID.

```
admin@LSR2# set protocols mpls ldp router-id 2.2.2.2
```

Step 6 Configure MPLS LDP transmission address under IPv4 address family.

```
admin@LSR2# set protocols mpls ldp ipv4-family discovery transport-address 2.2.2.2
```

Step 7 Configure LDP ordered label distribution control.

```
admin@LSR2# set protocols mpls ldp ordered-control
```

Step 8 Enable IP routing.

```
admin@LSR2# set ip routing enable true
```

Step 9 Commit the configuration.

```
admin@LSR2# commit
```

LSR 3

Step 1 Configure VLAN interface.

```
admin@LSR3# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 20
admin@LSR3# set l3-interface vlan-interface vlan20 address 20.20.20.22 prefix-length 24
admin@LSR3# set vlans vlan-id 20 l3-interface vlan20
admin@LSR3# set l3-interface loopback lo3 address 3.3.3.3 prefix-length 32
```

Step 2 Configure the OSPF protocol to advertise the network segments connected to each node's interfaces and the LSR's host routes.

```
admin@LSR3# set protocols ospf router-id 3.3.3.3
admin@LSR3# set protocols ospf network 20.20.20.0/24 area 0
admin@LSR3# set protocols ospf network 3.3.3.3/32 area 0
```

Step 3 Enable MPLS on the L3 interface.

```
admin@LSR3# set protocols mpls interface vlan20
```

Step 4 Enable MPLS on the L3 interface. Usually, both the incoming and outgoing interfaces of the packets need to enable MPLS. By default, MPLS is disabled on the L3 interface.

```
admin@LSR3# set protocols mpls ldp ipv4-family interface vlan20
```

Step 5 Configure MPLS router ID.

```
admin@LSR3# set protocols mpls ldp router-id 3.3.3.3
```

Step 6 Configure MPLS LDP transmission address under IPv4 address family.

```
admin@LSR3# set protocols mpls ldp ipv4-family discovery transport-address 3.3.3.3
```

Step 7 Configure LDP ordered label distribution control.

```
admin@LSR3# set protocols mpls ldp ordered-control
```

Step 8 Enable IP routing.

```
admin@LSR3# set ip routing enable true
```

Step 9 Commit the configuration.

```
admin@LSR3# commit
```

Verify the Configuration

- After the configuration is complete, run command **run show mpls ldp neighbor** on each LSR. From the show result, we can see that MPLS LDP state is "`OPERATIONAL`", indicating successful establishment of LDP session. Take LSR 2 as an example:

```
admin@LSR2# run show mpls ldp neighbor
AF   ID              State       Remote Address    Uptime
ipv4 1.1.1.1         OPERATIONAL 1.1.1.1           00:00:39
ipv4 3.3.3.3         OPERATIONAL 3.3.3.3           00:01:14
```

- After the configuration is complete, run command **run show mpls ldp binding** to verify label bindings.

```
admin@LSR2# run show mpls ldp binding
AF   Destination          Nexthop         Local Label Remote Label  In Use
ipv4 1.1.1.1/32           1.1.1.1         17          imp-null         yes
ipv4 2.2.2.2/32           0.0.0.0         imp-null    -                 no
ipv4 3.3.3.3/32           3.3.3.3         16          imp-null         yes
ipv4 10.36.15.0/24        1.1.1.1         imp-null    imp-null          no
ipv4 10.36.15.0/24        3.3.3.3         imp-null    imp-null          no
ipv4 20.20.20.0/24        3.3.3.3         imp-null    imp-null          no
ipv4 172.10.10.0/24       1.1.1.1         imp-null    imp-null          no
```

In the show result, the parameter "`In Use`" indicates whether the label binding entry is effective or not.

- **yes**: indicates the label binding entry is effective.
- **no**: indicates the label binding entry is ineffective.

RFC Lists for MPLS

The following table lists the RFC documents related to MPLS function.

RFC	Description
RFC 3031	Multiprotocol Label Switching Architecture
RFC 3032	MPLS Label Stack Encoding
RFC 3034	Use of Label Switching on Frame Relay Networks Specification
RFC 3036	LDP Specification
RFC 5036	LDP Specification
RFC 3215	LDP State Machine
RFC 5443	LDP IGP Synchronization

Lossless Network Configuration

- Lossless Network Introduction
- Application Scenarios
- Key Features of Lossless Network
- Configuring Priority-based Flow Control (PFC)
  - Enabling PFC Function
  - Configuring PFC Buffer
  - Configuring PFC Watchdog
  - Configuring PFC Deadlock Prevention
- Configuring Explicit Congestion Notification (ECN)
- Configuring Easy ECN
- PFC and ECN Statistical Reporting through gRPC
- Configuring Dynamic Load Balancing
- Typical Configuration Example of Lossless Network

Lossless Network Introduction

- Overview
- Advantages
- Versions of RoCE
- Supported Platforms
- Switch Configuration

Overview

Lossless networks are crucial for the implementation of RDMA over Converged Ethernet (RoCE), a network protocol that enables high-throughput and low-latency data communication between nodes in a network. RoCE leverages the advantages of Remote Direct Memory Access (RDMA) technology over standard Ethernet networks, making it highly suitable for applications requiring rapid data transfer and minimal latency, such as high-performance computing, distributed storage, AI deep learning model training and big data analytics.

Advantages

1. **Low Latency**: RoCE reduces the latency of data transfers by bypassing the CPU and the operating system in the data path, allowing direct memory-to-memory data transfers.
2. **High Throughput**: By enabling direct memory access, RoCE can achieve higher data transfer rates compared to traditional Ethernet communications.
3. **Efficient CPU Usage**: Because RoCE offloads data transfer tasks from the CPU, it frees up CPU cycles for other processing tasks, enhancing overall system performance.
4. **Ethernet Compatibility**: RoCE leverages the existing Ethernet infrastructure, making it cost-effective to deploy in data centers without requiring specialized networking equipment.

Versions of RoCE

There are two main versions of RoCE:

1. **RoCEv1**: This version operates at Layer 2 of the OSI model, meaning it is not routable beyond the local Ethernet network. It requires all devices to be in the same Ethernet broadcast domain.
2. **RoCEv2**: This version operates at Layer 3, making it routable over IP networks. RoCEv2 packets can traverse multiple subnets, allowing for greater scalability and flexibility in network design.

Supported Platforms

To achieve lossless network communication, high throughput, and low latency data exchange between nodes, features like PFC Watchdog, Explicit Congestion Notification (ECN), and Dynamic Load Balancing are only supported on **Trident3** and **Tomahawk3** platforms.

Switch Configuration

To effectively leverage RoCE in your network, configuring your switches properly is crucial. Here's the guide to configure lossless network on network switches, focusing on key features: PFC, PFC Watchdog, ECN and Dynamic Load Balancing (DLB).

- **Interface**
  - Enable with PFC on the required priority.
- **Global Configuration**

- Configure ECN via WRED
  - Enable WRED.
  - Set the maximum and minimum thresholds.
  - Set drop probability.
  - Enable ECN.
- Configure PFC Watchdog
  - Enable PFC on the interface before enabling PFC watchdog.
  - Enable PFC watchdog.
  - Configure the time interval of PFC deadlock detection.
  - Configure the restore time and restore action when PFC deadlock occurs.
- Configure Dynamic Load Balancing

Application Scenarios

Application Scenarios 1: High Performance Computing (HPC)

Application Scenarios 2: Distributed Storage

Application Scenarios 3: Artificial Intelligence (AI)

Lossless networks are utilized across various industries and applications due to its ability to provide low-latency, high-throughput communication. Here are some key use cases of lossless networks:

Application Scenarios 1: High Performance Computing (HPC)

Lossless networks are widely used in High Performance Computing (HPC) due to its ability to provide low-latency and high-throughput communication. These attributes are critical for HPC environments, which involve complex computational tasks requiring efficient data transfer between numerous computing nodes.

1. **Parallel Computing**:
   - **Inter-node Communication**: Lossless network is used for fast communication between nodes in a cluster, essential for parallel computing tasks where multiple nodes work on different parts of a problem simultaneously.
   - **MPI Acceleration**: Lossless network enhances the performance of MPI (Message Passing Interface) applications by reducing communication overhead.
2. **Distributed Databases**:
   - **Efficient Data Replication**: Lossless network facilitates high-speed data replication between database nodes, ensuring data consistency and high availability.
   - **Query Processing**: Faster data movement between nodes improves the performance of distributed query processing.
3. **Data Analytics and Machine Learning**:
   - **Large Dataset Handling**: Lossless network enables efficient handling of large datasets, which is crucial for big data analytics and machine learning applications.
   - **Model Training**: Accelerates the training of machine learning models by speeding up data transfer between compute nodes and storage systems.
4. **Scientific Simulations**:
   - **Real-time Data Sharing**: Scientific simulations often require real-time data sharing between nodes, which lossless network supports through its low-latency and high-throughput capabilities.
   - **Collaborative Research**: Facilitates collaborative research by enabling seamless data exchange and communication between geographically distributed research centers.

Application Scenarios 2: Distributed Storage

Lossless network is increasingly being applied in distributed storage systems due to its ability to provide low-latency and high-throughput data transfers. These features are crucial for distributed storage environments, which require efficient and reliable data movement between storage nodes.

1. **Distributed File Systems**:
   - **Fast Data Access**: Lossless network enhances the performance of distributed file systems like HDFS (Hadoop Distributed File System) by enabling fast data access and transfers between nodes.
   - **Efficient Data Replication**: Ensures that data replication between storage nodes is performed quickly and reliably, maintaining data consistency and availability.
2. **Object Storage**:
   - **High-Performance Object Storage**: Lossless network can be used to improve the performance of object storage systems like Ceph, which require efficient handling of large objects across distributed nodes.

- **Reduced Latency**: Low-latency data transfers ensure quick access to stored objects, enhancing the overall user experience and system performance.

3. **Block Storage**:
   - **Enhanced Block Storage Performance**: Lossless network improves the performance of block storage solutions by enabling low-latency access to storage blocks, which is crucial for applications requiring fast I/O operations.
   - **Efficient Volume Management**: Facilitates efficient volume management and data migration between storage devices.
4. **Software-Defined Storage (SDS)**:
   - **Improved SDS Efficiency**: Lossless network can enhance the efficiency of software-defined storage systems by enabling high-speed, low-latency communication between storage nodes and controllers.
   - **Scalable Storage Solutions**: Supports the scalability needs of SDS, allowing for seamless expansion and management of storage resources.

Application Scenarios 3: Artificial Intelligence (AI)

Lossless network is highly beneficial in AI environments, particularly for deep learning and large-scale AI workloads. The need for high-speed, low-latency communication between numerous GPUs or compute nodes makes lossless network an ideal choice for AI applications.

1. **Deep Learning Model Training**:
   - **Distributed Training**: Lossless network facilitates efficient communication between multiple GPUs or nodes during distributed training, reducing training time.
   - **Data Parallelism**: Enhances data parallelism by allowing seamless data exchange between nodes, ensuring that each node has the required data for training.
2. **Inference Serving**:
   - **Low-latency Inference**: Lossless network's low-latency capabilities are critical for real-time inference serving, enabling quick responses in AI-driven applications.
   - **Scalable Inference**: Supports scaling inference workloads across multiple nodes or GPUs, ensuring that large-scale inference tasks are handled efficiently.
3. **AI Data Processing Pipelines**:
   - **High-throughput Data Transfers**: Lossless network can handle the high-throughput data transfers required in AI data processing pipelines, such as ETL (Extract, Transform, Load) operations.
   - **Streamlined Data Movement**: Ensures efficient data movement between storage and compute nodes, enhancing the performance of data preprocessing steps in AI workflows.
4. **Big Data Analytics**:
   - **Accelerated Analytics**: By providing high-speed data transfers, lossless network accelerates the analytics processes that feed into AI models, improving the overall pipeline efficiency.
   - **Integration with Hadoop and Spark**: Enhances the performance of big data frameworks like Hadoop and Spark, which are often used in conjunction with AI workloads.

Key Features of Lossless Network

Lossless network is a powerful networking protocol designed to enable high-performance, low-latency data transfers over Ethernet networks. By leveraging RDMA technology, lossless network offers significant benefits for various high-demand applications, making it a crucial component in modern data centers, high-performance computing environments, and cloud services. Its ability to utilize existing Ethernet infrastructure makes it a cost-effective solution for enhancing network performance.

Lossless network switches are designed to support the unique requirements of RDMA, providing low-latency and high-throughput communication over Ethernet networks. Here are the key technologies and features that are crucial for lossless network switches:

Priority Flow Control (PFC)

Priority Flow Control (PFC) is a network protocol designed to manage congestion on Ethernet networks by allowing for the independent pausing of traffic based on priority levels. It is part of the IEEE 802.1Qbb standard and is particularly useful in data center environments where different types of traffic need to be handled with varying degrees of urgency.

PFC is a critical technology for managing congestion in Ethernet networks, particularly in data center environments. By enabling traffic differentiation and providing lossless transport for high-priority traffic, PFC helps maintain performance and reliability for critical applications.

PFC Watchdog

PFC Watchdog is a critical component in Ethernet networks that use Priority Flow Control to manage congestion. By detecting and mitigating PFC deadlocks, it ensures that the network remains stable and performs optimally. This mechanism is particularly important in data centers and other environments where maintaining high performance and reliability is crucial.

Explicit Congestion Notification (ECN)

Explicit Congestion Notification (ECN) is an effective mechanism for managing network congestion by marking packets instead of dropping them. It is an extension of the IP and TCP protocols, enhancing the way congestion is managed by marking packets instead of discarding them. It helps improve network performance, reduce packet loss, and maintain high throughput, making it especially valuable in data centers and for real-time applications.

Dynamic Load Balance

Dynamic Load Balancing is a network management technique used to distribute network traffic across multiple paths or resources dynamically. Unlike static load balancing, which assigns fixed routes or resources to handle traffic, dynamic load balancing adjusts traffic distribution in real-time based on current network conditions.

It is a vital network management technique that optimizes performance, scalability, and reliability by dynamically distributing traffic across multiple paths or resources. By adapting to changing network conditions in real-time, dynamic load balancing ensures efficient resource utilization and enhances overall network performance and resilience.

In the following sections, we will explain the details of what they are, how they work, and how to configure.

Configuring Priority-based Flow Control (PFC)

- Enabling PFC Function
- Configuring PFC Buffer
- Configuring PFC Watchdog
- Configuring PFC Deadlock Prevention

Enabling PFC Function

Overview

Priority-based Flow Control (PFC) is a type of flow control mechanism. The advantage of PFC over traditional flow control mechanisms is that PFC provides flow control based on per-code-point (priority). In other words, PFC offers a more granular form of flow control. This means that if traffic from one particular priority suffers from congestion, only that traffic is paused until the congestion clears, while traffic for other priorities continues unhindered. On each physical port, there are 8 (0 to 7) Class of Service (CoS) queues. If congestion is detected on the egress physical port, the ingress port will send a PAUSE frame to the transmitting node to pause transmission until the receiving node is ready to accept packets again. PFC applies only to packets entering a port.

PFC has a higher priority than traditional flow control. For example, if both flow control and PFC are configured on the same port, PFC will take precedence over traditional flow control.

PFC uses the IEEE 802.1p CoS values in the IEEE 802.1Q VLAN tag to generate the flow control frame with the corresponding priority on the ingress physical port when the egress physical port suffers congestion. This indicates that the ingress port requires CoS classifier configuration.

Key Features of PFC

1. **Lossless Transmission**: PFC ensures lossless transmission for high-priority traffic classes by pausing traffic when congestion is detected, preventing packet loss.
2. **Per-Priority Flow Control**: Unlike traditional Ethernet flow control, which applies to all traffic on a link, PFC operates on individual traffic priorities, allowing selective flow control.
3. **Congestion Management**: By preventing packet loss for specific traffic classes, PFC helps manage congestion and improve overall network performance.

Working Mechanism of PFC

PFC operates using the following key components and steps:

1. **Traffic Classification**: Network traffic is classified into different priorities based on the IEEE 802.1p standard, which defines eight priority levels (0-7). Each priority level corresponds to a specific type of traffic, such as storage, voice, or best-effort data.
2. **Priority Mapping**: The switch maps traffic to these priority levels using VLAN tags (802.1Q) or Differentiated Services Code Point (DSCP) values. Each priority level is associated with a separate queue within the switch.
3. **Congestion Detection**: When a switch detects congestion in one of its priority queues (e.g., due to high traffic volume or insufficient buffer space), it generates a PFC frame for that specific priority level.
4. **PFC Frame Transmission**: The PFC frame, also known as a PAUSE frame, is sent to the upstream device (e.g., another switch or a network interface card in a server). This frame instructs the upstream device to pause the transmission of traffic for the specified priority level.
5. **Traffic Pause**: Upon receiving the PFC frame, the upstream device temporarily stops sending traffic of the specified priority to the congested switch. Other traffic classes (priorities) continue to flow without interruption, ensuring that only the affected traffic is paused.
6. **Congestion Alleviation**: The switch continues to process and forward the paused traffic until the congestion is alleviated. Once the buffer space is available, the switch sends another PFC frame to the upstream device to resume the paused traffic flow.
7. **Resume Transmission**: The upstream device resumes sending traffic for the previously paused priority, restoring normal traffic flow.

Advantages of PFC

1. **Improved Performance**: By preventing packet loss for high-priority traffic, PFC ensures that critical applications, such as storage and real-time communications, perform reliably.

2. **Enhanced Network Efficiency**: PFC allows network devices to manage congestion more effectively, reducing the likelihood of network bottlenecks and improving overall network efficiency.
3. **Coexistence of Traffic Types**: PFC enables different types of traffic to coexist on the same network infrastructure without interfering with each other, supporting the convergence of storage, data, and voice traffic.

Restrictions and Guidelines

When you configure PFC, follow these restrictions and guidelines:

- It is essential to ensure that the PFC functionality is enabled on all ports through which the packets flow.
- To prevent packet loss due to congestion during transmission, please configure the same PFC settings on all ports through which the packets flow.

Procedure

Step 1 Configure PFC Profile.

By default, PFC is enabled.

PFC is disabled when drop value is set to true and enabled when drop value is set to false. The default value of drop is false.

set class-of-service pfc-profile <*pfc-profile-name*> **code-point** <*cos*> **drop** <**true** | **false**>

Step 2 Apply PFC profile to the interface.

set class-of-service interface <*interface-name*> **pfc-profile** <*pfc-profile-name*>

Step 3 Commit the configuration.

commit

Show PFC Frame Statistics on Port

After complete the configuration, the command **run show class-of-service interface** `<` *interface-name*> can be used to show the class of service statistics information on specified interface.

Configuration Example

The following commands complete the configurations:

- Configure PFC profile `pfc1`.
- Apply PFC profile to the port `ge-1/1/1`.

```
admin@PICOS# set class-of-service pfc-profile pfc1
admin@PICOS#set class-of-service interface ge-1/1/1 pfc-profile pfc1
```

- Show the class of service statistics information on specified interface.

The class 0~7 in PFC frame corresponds to the following "802.1P" item. The value of ”RxPFC“ item will be incremented by 1 if ge-1/1/1 receives a PFC frame. The value of ”TxPFC“ item will be incremented by 1 if ge-1/1/1 sends out a PFC frame.

```
admin@PICOS# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1

802.1P         Priority Flow Control    RxPFC              TxPFC
-----------    ---------------------    ---------------    ---------------
0              false                     0                  500
1              false                     0                  0
```

```
2              false                     0                 71
3              false                     0                 0
4              false                     0                 0
5              false                     0                 0
6              false                     0                 102
7              false                     0                 0
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule               Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

Configuring PFC Buffer

Overview

The buffer is configured to implement traffic control and PFC watchdog, which is based on interface and priority queue. The storage space of each interface is divided into different buffers independently and a certain action will be executed after the number of accumulated packets reaches the buffer threshold (the unit is cell).

- **Guaranteed**: the dedicated buffer available for a specified queue. This buffer space cannot be used by other queues.
- **Shared**: the public buffer available for all queues. The shared buffer will be occupied when the guaranteed buffer reaches the threshold.
- **Headroom**: the maximum number of cell resources available for packets with a specific 802.1p priority. When the occupied shared buffer reaches the threshold, the packets will be saved in the headroom buffer.

Threshold and Execution Action

After the PFC function is enabled, the default storage space is available for a specified queue of an interface. To flexibly control the PFC function and make good use of the storage space, you can configure the thresholds for different buffer types and the correspongding action will be executed. The detailed information is shown as below.

Figure 1. Communication between upstream and downstream switches

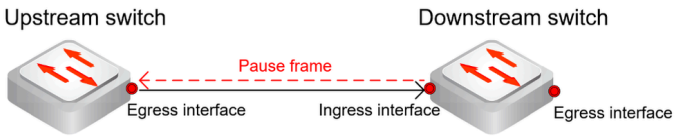
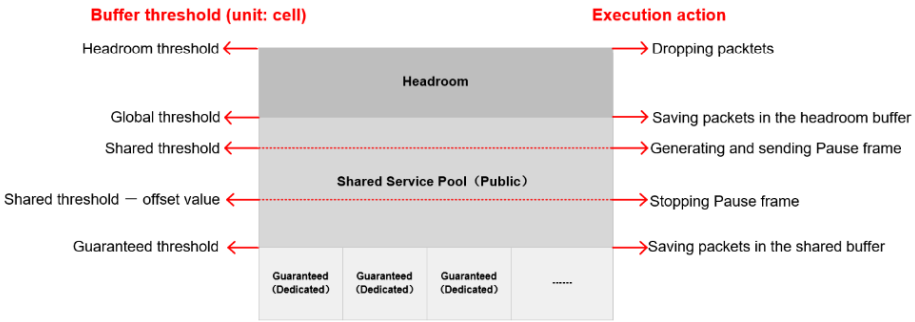


Figure 2. Buffer threshold and execution action of an interface



1. Initially, the packets of a specified queue on an interface are saved in the guaranteed buffer. When the occupied space is higher than the guaranteed buffer threshold, the shared buffer will be occupied.
2. When the occupied space is higher than the shared buffer threshold, the ingress interface and egress interface of the downstream switch will execute different actions.

   a) For the ingress interface, it will generate and send Pause frames to the egress interface of the upstream switch to stop sending packets. The Pause frames will stop being generated when the occupied space is reduced to a certain level (the shared threshold minus the offset value). When the occupied space is higher than the global threshold, the packets will be saved in the headroom buffer.

   b) For the egress interface, the packets will be directly saved in the headroom buffer.

3. When the occupied space is higher than the headroom buffer threshold, the packets will be dropped.

Restrictions and Guidelines

When you configure PFC buffer, follow these restrictions and guidelines:

- PFC should be enabled on the interface before configuring PFC buffer.
- Currently, the PFC buffer is only supported on **Trident3-X5, Trident3-X7**, **Tomahawk3** and **Tomahawk5** platforms.
- The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Procedure

Step 1 Enable PFC on the interface before configuring PFC buffer.

set class-of-service pfc-profile <*pfc-profile-name*> [**code-point** <*cos*> **drop** <**true** | **false**>]

set class-of-service interface <*interface-name*> **pfc-profile** <*pfc-profile-name*>

Step 2 Set the upper threshold of guaranteed buffer for a PFC queue on the **ingress** interface. When the guaranteed buffer threshold is reached, the packets will be saved in the shared service pool.

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **guaranteed** <*value*>

Step 3 Set the upper threshold of shared buffer for a PFC queue on the **ingress** interface. When the occupied buffer space exceeds the specified threshold, the Pause frame will be generated and sent to the egress interface. You can specify the threshold in the static (a fixed value) or dynamic (percentage) way.

Only one way can be configured, or the error prompt will appear.

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **shared-ratio** <*value*>

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **threshold** <*value*>

Step 4 Set the offset value of shared buffer for a PFC queue on the **ingress** interface. The Pause frames will stop being generated when the occupied space is reduced to a certain level (the upper threshold minus the offset value).

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **reset-offset** <*value*>

Step 5 Set the global threshold of shared buffer for a PFC queue on all **ingress** interfaces. When the global threshold is reached, the packets will be saved in the headroom buffer.

set interface ethernet-switching-options buffer service-pool <*pool-id*> **threshold** <*value*>

Step 6 Set the upper threshold of headroom buffer for a PFC queue on the **ingress** interface. When the headroom buffer threshold is reached, the interface will drop received packets.

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **headroom** <*value*>

Step 7 Set the upper threshold of shared buffer for a PFC queue on the **egress** interface of the downstream switch. When the occupied buffer space exceeds the specified threshold, the packets will be saved in the headroom buffer. You can specify the threshold in the static (a fixed value) or dynamic (percentage) way.

Only one way can be configured, or the error prompt will appear.

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer egress-queue** <*queue-id*> **shared-ratio** <*value*>

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer egress-queue** <*queue-id*> **threshold** <*value*>

Step 8 Commit the configuration.

commit

Configuring PFC Watchdog

- Understanding PFC Deadlock
- PFC Watchdog Mechanism
- Key Components and Functions of PFC Watchdog
- Restrictions and Guidelines
- Configuring PFC Watchdog
  - Procedure
- Verifying the Configuration

Priority Flow Control (PFC) is a mechanism used in data center networks to ensure lossless transmission for high-priority traffic by pausing traffic when congestion is detected. While PFC helps in managing traffic congestion, it can potentially lead to a situation known as a **PFC deadlock**. To address this issue, network devices employ a **PFC watchdog** mechanism to detect and mitigate PFC deadlocks.

Understanding PFC Deadlock

A PFC deadlock occurs when multiple devices in a network are continuously sending PFC pause frames to each other, leading to a situation where traffic is indefinitely paused, causing a complete halt in data transmission. This deadlock can severely impact network performance and application availability.

PFC Watchdog Mechanism

The PFC watchdog is designed to detect and resolve PFC deadlocks. It monitors the duration of PFC pause frames and takes corrective actions if a potential deadlock is detected.

PFC Deadlock Detection and Recovery

By configuring the PFC deadlock detection function, the device can periodically check if it is in a PFC deadlock state. When the device detects a PFC deadlock, it will automatically resolve the deadlock within the recovery period. The system will resume sending traffic for the corresponding priority queue, or it can configure to discard the traffic for the corresponding priority queue. After the recovery period, the normal PFC flow control mechanism will be restored. If a deadlock is detected again during the next detection cycle, a new cycle of deadlock recovery procedures will be initiated.

PFC Deadlock Control Process

If the above deadlock recovery procedures are ineffective and PFC deadlocks continue to occur, users can configure the system to forcibly enter the deadlock control process after a certain number of deadlocks within a specified period. For example, if PFC deadlocks are triggered a certain number of times within a set period, indicating a high risk of frequent deadlocks in the network, the system will enter the deadlock control process. At this point, the device will automatically disable the PFC function to ensure normal packet forwarding and to clear the deadlock state.

After the PFC deadlock state is resolved, users have to restore the PFC deadlock detection function manually. Restoring the PFC deadlock detection function reactivates the PFC feature.

Key Components and Functions of PFC Watchdog

1. **Monitoring PFC Pause Frames**: The PFC watchdog continuously monitors the network for PFC pause frames. It keeps track of the duration for which these frames are active for each priority class on each port.

   The following command can be used to enable PFC watchdog functionality:

   set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable** <**true** | **false**>

2. **Timeout Threshold**: A configurable timeout threshold is set for PFC pause frames. If a pause frame for a specific priority exceeds this threshold, it indicates a potential deadlock situation.

   The detect timer can be configured by the following commands:

   set class-of-service pfc-watchdog granularity <**10** | **100**>

   set class-of-service pfc-watchdog code-point <*cos*> **detect-interval** <*detect-interval*>

3. **Deadlock Detection**: When the duration of a PFC pause frame surpasses the timeout threshold, the PFC watchdog triggers a deadlock detection process. This process identifies the ports and priority classes involved in the deadlock.
4. **Restore Actions**: Once a potential deadlock is detected, the PFC watchdog takes restore actions to break the deadlock. These actions typically include:

   - **Forward**: During the PFC deadlock recovery process, the received PFC PAUSE frame will be ignored, and the internal scheduler will resume forwarding the traffic.
   - **Drop**: Drops received data packets.

   After a predefined period, the PFC watchdog re-enables PFC for the affected priority class. This period allows the network to stabilize and clear any residual congestion that could cause another deadlock.

   The restore action can be configured by the following commands:

   set class-of-service pfc-watchdog restore-action <**forward** | **drop**>

   set class-of-service pfc-watchdog code-point <*cos*> **restore-interval** <*restore-interval*>

5. **Set the Recovery Mode for a Deadlocked Port**

   The following command can be used to configure the restore mode, the default is automatic recovery.

   set class-of-service interface <*interface-name*> **pfc-watchdog restore-mode <manual | auto>**

   The two different restore modes **Manual** and **Auto** represent different deadlock detection processes and different PFC deadlock recovery methods:

   - **Auto**

   When PFC watchdog functionality is enabled and the restore mode for a port is set to **Auto** recovery, the PFC watchdog continuously monitors the PFC activity on the port. If deadlocks repeatedly occur and the count exceeds the configured threshold within the specified time period, the system determines that the port is in an unstable state and will automatically disable the PFC feature to prevent further network disruption.

   Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

   run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

   - **Manual**

   When PFC watchdog functionality is enabled and the restore mode for a port is set to **Manual** recovery, the PFC watchdog continuously monitors the PFC activity on the port, once a PFC deadlock occurs, the PFC function on that port will be automatically disabled.

   Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

   run clear class-of-service interface <*interface-name*> **pfc-watchdog manual**

   This ensures that persistent deadlocks do not degrade network performance.

6. **Set the Maximum Number of PFC Deadlocks within a Specified Period**
   When the recovery mode for a port is set to automatic recovery, and the number of PFC deadlocks reaches the upper limit within the specified period, the PFC function on that port will be disabled. In this case, users need to do step 7 to re-enable PFC function.

set class-of-service pfc-watchdog threshold period <*time*>

set class-of-service pfc-watchdog threshold count <*count*>

7. **Re-enabling PFC and PFC Watchdog**

   • When a port experiences a deadlock and the recovery mode is set to manual, this command needs to be run to re-enable the PFC function:

   run clear class-of-service interface <*interface-name*> **pfc-watchdog manual**

   • When the deadlock limit is configured and the port deadlock reaches the upper limit, the reset command needs to be executed to re-enable the PFC function:

   run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

Restrictions and Guidelines

When you configure PFC watchdog, follow these restrictions and guidelines:

- PFC should be enabled on the interface before enabling PFC watchdog.
- PFC watchdog is only supported on **Trident3-X5, Trident3-X7**, **Tomahawk3** and **Tomahawk5** platforms.

Configuring PFC Watchdog

Procedure

Step 1 Enable PFC on the interface before enabling PFC watchdog.

set class-of-service pfc-profile <*pfc-profile-name*> [**code-point** <*cos*> **drop** <**true** | **false**>]

set class-of-service interface <*interface-name*> **pfc-profile** <*pfc-profile-name*>

Step 2 Enable PFC watchdog. By default, PFC watchdog is disabled.

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable** <**true** | **false**>

Step 3 (Optional) Configure the time interval of PFC deadlock detection. The default detection timer is 1.5 seconds. The value of detection time = **granularity** x **detect-interval**.

set class-of-service pfc-watchdog granularity <**10** | **100**>

set class-of-service pfc-watchdog code-point <*cos*> **detect-interval** <*detect-interval*> (On **Trident3** platforms)

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **detect-interval** <*detect-interval*> (On **Tomahawk3** platforms)

Step 4 (Optional) Configure the restore time and restore action when PFC deadlock occurs. The default restore action is forward. The restore time = **granularity** x **restore-interval**.

set class-of-service pfc-watchdog restore-action <**forward** | **drop**>

set class-of-service pfc-watchdog code-point <*cos*> **restore-interval** <*restore-interval*> (On **Trident3** platforms)

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **restore-interval** <*restore-interval*> (On **Tomahawk3** platforms)

Step 5 (Optional) Set the restore mode for a deadlocked port. If this command is not configured, the default is automatic recovery.

set class-of-service interface <*interface-name*> **pfc-watchdog restore-mode <manual | auto>**

Step 6 (Optional) Set the maximum number of PFC deadlocks within a specified period.

When the recovery mode for a port is set to automatic recovery, and the number of PFC deadlocks reaches the upper limit within the specified period, the PFC function on that port will be disabled. In this case, users need to do step 8 to re-enable PFC function.

set class-of-service pfc-watchdog threshold period <*time*>

set class-of-service pfc-watchdog threshold count <*count*>

Step 7 Commit the configuration.

commit

Step 8 (Optional) Re-enable PFC and PFC watchdog.

• When a port experiences a deadlock and the recovery mode is set to manual, this command needs to be run to re-enable the PFC function:

run clear class-of-service interface <*interface-name*> **pfc-watchdog manual**

• When the deadlock limit is configured and the port deadlock reaches the upper limit, the reset command needs to be executed to re-enable the PFC function:

run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

Verifying the Configuration

- After the configuration, use command **run show pfc-watchdog config** to view the configuration information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog config
    PORT    ACTION      QUEUE    DETECTION TIME   RESTORATION TIME
----------  -----------   ------------  ----------------  ------------------
te-1/1/25     drop       5             150               150
                    6             150               150
                    7             120               110
```

- Use command **run show pfc-watchdog stats** to view the statistics information about PFC watchdog, including the number of PFC pause storms that have been detected and restored, as well as the number of packets that have been dropped, on the PFC queues on an interface.

```
admin@PICOS# run show pfc-watchdog stats
       QUEUE       STATUS    STORM DETECTED/RESTORED        TX OK/DROP    TX LAST OK/DROP
------------  -----------  ------------------------  ----------------  -------------------
te-1/1/25:5       stormed                       9/8      82072626556/0  32053822365/0
te-1/1/25:6       stormed                       9/8      31504345475/0  32053822365/0
te-1/1/25:7   operational                       0/0                0/0  0/0
```

In the show result,

- **STATUS**: The status of PFC watchdog. The value could be **operational** or **stormed**.
  - **operational**: Currently under detection, no deadlock found.
  - **stormed**: Currently in a deadlock state.
- **STORM DETECTED**: Queue deadlock counter.
- **STORM RESTORED**: Queue restore counter.

- **TX DROP** and **TX LAST DROP**: Number of Tx packets dropped due to PFC deadlock.
- **TX OK** and **TX LAST OK**: Number of Tx packets transmitted during deadlock (Forward action).

Configuring PFC Deadlock Prevention

- Overview
- Restrictions and Guidelines
- Configuring PFC Deadlock Prevention
  - Procedure
  - Configuration Example

Overview

Consider a data center running RoCE (RDMA over Converged Ethernet) traffic for high-performance computing workloads. These workloads require low-latency, lossless traffic flow, which PFC is used to enforce. However, as network congestion builds up, PFC pause frames are triggered, potentially leading to a deadlock if multiple paths become blocked.

By employing a PFC deadlock prevention solution, the network can identify RoCE flows that are prone to triggering deadlocks. The solution adjusts the queue priorities so that other critical flows are not blocked, and it reduces the load on congested paths. This prevents the generation of circular wait conditions and ensures the smooth operation of high-priority traffic, ensuring that business-critical applications continue to function smoothly without being interrupted by PFC-induced deadlocks.

How PFC Deadlock Prevention Works in Practice

1. **Monitoring and Analytics**

Figure 1. PFC Hook Flows

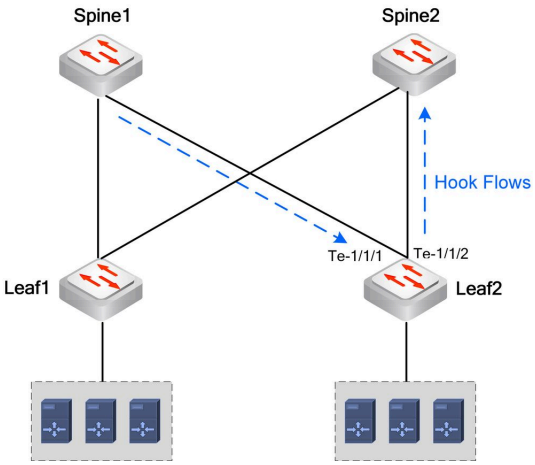


Figure 1 shows a CLOS network, it is a highly scalable and high-performance switching network commonly used in modern data centers. It is a multi-stage network topology, typically with multiple leaf and spine switches, which is designed to handle massive amounts of data with minimal latency and is often used to interconnect thousands of servers. Usually, PFC is deployed to manage flow control and avoid packet loss.

PFC Uplink Port Group

As shown in **Figure 1**, interfaces Te-1/1/1 and Te-1/1/2 are the uplinks connecting Leaf2 to the spines. They are added to the PFC uplink port group so that the system treats them collectively, allowing the device to manage them as a single entity when assessing traffic flow and PFC behavior.

High-Risk Hook Flow

As shown in **Figure 1**, when a leaf device detects that the same business flow (i.e., a specific set of traffic identified by its characteristics, such as source/destination IP, port, etc.) is traversing multiple interfaces within the PFC uplink port group, it marks this flow as a high-risk

hook flow.

When a high-risk hook flow generates congestion across multiple interfaces (uplinks), PFC pause frames may be issued by the leaf to its upstream spine switches. If both interfaces in the uplink group send pause frames, and the upstream spine switches are also congested, it can result in a circular wait scenario (deadlock). The switches are effectively waiting for each other to release the paused traffic, leading to a network stall.

The **Deadlock Prevention** solution proactively monitors the data center network for high-risk hook flow that may lead to the generation of PFC pause frames.

2. **Dynamic Queue Management**

After the device receives the packet, it modifies the DSCP value and the corresponding dot1p priority of the packet, so that the packet is forwarded in the new dot1p priority queue using the new DSCP value.

The **PFC deadlock prevention** function in CLOS networks works by creating **PFC uplink port groups** that combine uplink interfaces on leaf devices together. The system detects high-risk flows that traverse these grouped uplinks and identifies them as potential deadlock triggers (high-risk hook flows). By preemptively modifying queue priorities and managing these flows, the system prevents deadlocks from occurring, ensuring the stability and efficiency of data center networks.

Restrictions and Guidelines

When you configure PFC deadlock prevention, follow these restrictions and guidelines:

- PFC Deadlock Prevention is only supported on **Trident3-X5**, **Trident3-X7**, **Tomahawk3** and **Tomahawk5** platforms.
- To ensure proper functioning, it is important that if any Equal-Cost Multi-Path (ECMP) output interfaces exist within the PFC uplink port group, **all of these ECMP interfaces** must be included in the group. Failing to do so may result in incorrect queue switching for Layer 3 traffic on the PFC uplink port group interfaces, leading to unexpected modifications of the DSCP (Differentiated Services Code Point) values. This could impair traffic handling and potentially lead to inefficiencies or incorrect prioritization.
- Each device supports only one PFC uplink port group.

Configuring PFC Deadlock Prevention

Procedure

Step 1 Create a PFC uplink port group.

set class-of-service interface <*interface-name*> **pfc-uplink-group** <*group-name*>

Step 2 Modify the queue priority of hook flow packets that match the PFC uplink port group and the original DSCP value.

set class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **to-code-point** <*queue*>

Step 3 Modify the queue priority of hook flow packets that match the PFC uplink port group and the original DSCP value. If this command is not configured, it means the DSCP value carried by the packets will not be adjusted.

set class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **dscp** <*value*>

> **NOTE**:
>
> When configuring on the Trident3-X5 and Trident3-X7 platforms, the configurations in step 2 and step 3 both need to be configured and submitted in the same commit.

Step 4 Commit the configuration.

commit

Configuration Example

The following commands complete the configurations:

- Create a PFC uplink port group group1.
- Modify the queue priority to 4 and DSCP value to 48 of the hook flow packets that match the PFC uplink port group group1 and the original DSCP value 32.

```
admin@PICOS# set class-of-service interface te-1/1/1 pfc-uplink-group group1
admin@PICOS# set class-of-service interface te-1/1/2 pfc-uplink-group group1
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 to-code-point 4
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 dscp 48
admin@PICOS# commit
```

Configuring Explicit Congestion Notification (ECN)

- Overview
  - How ECN Works
  - Key Concepts
  - ECN Field in the IP Header
  - ECN Operation
  - Advantages of ECN
- Restrictions and Guidelines
- Configuring ECN via WRED
  - Procedure
  - Verify Configuration
  - Monitor and Adjust
- Configuration Example
- Test Recommended Configuration

Overview

Explicit Congestion Notification (ECN) is a network protocol feature that allows end-to-end notification of network congestion without dropping packets. It is an extension of the IP and TCP protocols, enhancing the way congestion is managed by marking packets instead of discarding them.

How ECN Works

ECN works by marking packets instead of dropping them when network devices detect congestion. This approach allows the sender to reduce its transmission rate proactively, improving overall network performance and reducing packet loss.

Key Concepts

1. **ECN-Capable Transport (ECT)**: Indicates that the endpoints are ECN-aware and can handle ECN markings.
2. **Congestion Experienced (CE)**: Indicates that the network is experiencing congestion.
3. **TCP ECN Echo (ECE)**: A TCP flag used to notify the sender that the receiver has received a packet marked with CE.
4. **Congestion Window Reduced (CWR)**: A TCP flag used by the sender to indicate that it has reduced its congestion window in response to receiving an ECE flag.

ECN Field in the IP Header

ECN uses two bits in the IP header, known as the ECN field, to signal congestion information:

- **00**: Not ECN-Capable Transport (Non-ECT)
- **01**: ECN Capable Transport (ECT(1))
- **10**: ECN Capable Transport (ECT(0))
- **11**: Congestion Experienced (CE)

ECN Operation

1. **Negotiation**: During the TCP three-way handshake, both endpoints negotiate the use of ECN. If both support ECN, they set the appropriate flags in their SYN packets.

2. **Packet Marking**: When an ECN-capable router detects congestion, it marks packets instead of dropping them. It sets the ECN field in the IP header to CE (11).
3. **Receiver Notification**: The receiver detects the CE marking and sets the ECE flag in the TCP header of its acknowledgment (ACK) packets.
4. **Sender Adjustment**: Upon receiving an ACK with the ECE flag, the sender reduces its transmission rate and sets the CWR flag in subsequent packets to indicate that it has responded to the congestion notification.

Therefore, it is necessary to reasonably set the ECN thresholds so that the buffer space between the ECN thresholds and PFC thresholds can accommodate the traffic sent during the time after the ECN congestion marking and before the source end slows down. This helps to avoid triggering PFC flow control as much as possible.

Advantages of ECN

1. **Reduced Packet Loss**: By marking packets instead of dropping them, ECN helps in avoiding packet loss, which is particularly beneficial for applications sensitive to packet drops, such as real-time video or voice.
2. **Improved Network Efficiency**: ECN allows for more efficient use of network resources by preventing congestion before it becomes severe enough to cause packet drops.
3. **Better Performance**: By avoiding packet loss, ECN can lead to better overall performance for TCP connections, resulting in higher throughput and lower latency.
4. **Smooth Traffic Flow**: ECN provides a mechanism for more graceful handling of congestion, leading to smoother traffic flow and improved end-user experience.

Restrictions and Guidelines

When you configure ECN, follow these restrictions and guidelines:

- To use ECN, both the network devices (such as routers and switches) and the endpoints (such as servers and clients) must support ECN.

Configuring ECN via WRED

On PICOS switches, ECN is used in conjunction with Weighted Random Early Detection (WRED) to provide early signals of congestion to avoid packet loss and improve network performance.

WRED is an active queue management (AQM) mechanism that selectively drops packets based on the average queue length, helping to manage congestion before the queue becomes full. When combined with ECN, WRED can mark packets instead of dropping them when congestion is detected.

Procedure

Step 1 Enable WRED.

set interface gigabit-ethernet <*interface-name*> **wred queue** <*queue-value*> **enable** <**true** |**false**>

Step 2 Set the maximum and minimum thresholds.

set interface gigabit-ethernet <*interface-name*> **wred queue** <*queue-value*> **max_thresh** <*max_thresh*>

set interface gigabit-ethernet <*interface-name*> **wred queue** <*queue-value*> **min_thresh** <*min_thresh*>

Step 3 Set drop probability.

set interface gigabit-ethernet <*interface-name*> **wred queue** <*queue-value*> **drop_probability** <*int*>

Step 4 Enable ECN.

set interface gigabit-ethernet <*interface-name*> **wred queue** <*queue-value*> **ecn_thresh** <*int*>

Step 5 Commit the configuration.

commit

Key Configuration Parameters

- **Min_Thresh**: The minimum average queue size at which WRED starts to mark packets.
- **Max_Thresh**: The maximum average queue size at which WRED starts to drop packets with the configured **Drop_Probability**.
- **Drop_Probability**: The probability that a packet will be marked with ECN when the average queue size is between the min and max thresholds.

Verify Configuration

Use the command **run show interface gigabit-ethernet** <*interface-name*> **wred** to check the settings of ECN and WRED .

Monitor and Adjust

Monitor the network to ensure that ECN marking and WRED are effectively managing congestion. Adjust the thresholds and probabilities as needed to optimize performance.

Configuration Example

The following commands complete the configurations:

- Enable WRED on queue 0 of interface ge-1/1/3;
- Set the maximum threshold to 400 and the minimum threshold to 200 on queue 0 of interface ge-1/1/3;
- Set the drop probability to 50% on queue 0 of interface ge-1/1/3;
- Enable ECN (Explicit Congestion Notification) on queue 0 of interface ge-1/1/3.

```
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 wred queue 0 enable true
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 wred queue 0 max_thresh 400
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 wred queue 0 min_thresh 200
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 wred queue 0 drop_probability 50
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 wred queue 0 ecn_thresh 1
admin@PICOS# commit
```

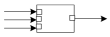
Show the WRED information of the specified interface.

```
admin@PICOS# run show interface gigabit-ethernet ge-1/1/3 wred
Queue Num    Min Thresh   Max Thresh   Drop Probability    ECN Thresh      Status
----------   ----------   ----------   ----------------    -----------     ----------
0              200            400            50%             Enabled        Enabled
1              0              0              0%              Disabled       Disabled
2              0              0              0%              Disabled       Disabled
3              0              0              0%              Disabled       Disabled
4              0              0              0%              Disabled       Disabled
5              0              0              0%              Disabled       Disabled
6              0              0              0%              Disabled       Disabled
7              0              0              0%              Disabled       Disabled
```

Test Recommended Configuration

Configuring ECN thresholds properly is crucial for ensuring optimal network performance, which helps in managing congestion proactively, leading to improved network performance, reduced packet loss, and lower latency.Testing recommended configurations involves setting specific parameters for ECN to manage congestion effectively and then evaluating the performance outcomes.

In the Lab, we use network simulation tools to create a controlled environment for testing. Simulate various traffic patterns and congestion scenarios to test how the network handles congestion. The table below provides recommended configuration values to prevent packet loss and avoid triggering the PFC threshold.

Test Method	Switch Port MTU	Switch Egress Port Link Bandwidth	ECN Min Threshold (Bytes)	ECN Max Threshold (Bytes)	Probability
 Three Ingress Port to One Egress Port	9000	99.75G	80000	8000000	80
 Three Ingress Port to One Egress Port	4096	97.68G	1000000	30000000	50
 Three Ingress Port to One Egress Port	9000	99.75G	1000000	32000000	50

Users have to continuously monitor network performance and ECN marking rates. Make dynamic adjustments to the ECN thresholds as needed to respond to changing network conditions.

Configuring Easy ECN

- Overview
- Configuration Notes and Constraints
- Configuring Easy ECN
  - Example

Overview

The Easy ECN feature streamlines the traditionally complex configuration of Explicit Congestion Notification (ECN) by eliminating the need for manual setup of interface queues, WRED (Weighted Random Early Detection) policies, thresholds, and drop probabilities. In standard ECN configurations, users need to configure multiple parameters, such as:

- **Enabling ECN** on specific interface queues, ensuring that the network is aware of which traffic classes should use ECN.
- **Setting WRED thresholds**, which determine at what point packets will be marked or dropped based on queue depth.
- **Configuring the maximum packet drop probability**, dictating how likely a packet is to be dropped when congestion is high.

Easy ECN simplifies all of these by allowing users to configure ECN with just a single command, focusing on the network's traffic optimization strategy.

By using the command **set class-of-service easy-ecn mode <throughput-first | latency-first>**, network administrators can efficiently configure ECN with a focus on either throughput or latency globally for all the interface queues, without needing to manually set all the individual parameters for each interface queue. This simplified approach not only saves time but also ensures more consistent and effective congestion management.

1. **Throughput-first Mode:** This mode prioritizes maximizing the amount of data transferred across the network, making it ideal for use cases such as bulk data transfers or content delivery systems. It dynamically adjusts traffic flow to ensure that congestion management does not overly restrict throughput, while still using ECN to prevent excessive congestion.

   In this mode, the threshold for marking packets is set relatively high. This allows for larger buffers to accumulate before marking occurs, reducing the chances of packet drops and enabling more traffic to be handled.

2. **Latency-first Mode:** This mode prioritizes minimizing latency, ensuring that packets experience the least possible delay. This is particularly important for real-time applications such as VoIP, video conferencing, or online gaming, where even small delays can negatively impact performance.

   In this mode, the ECN marking threshold is set lower, meaning packets will be marked sooner when congestion starts to build up. This results in less buffer buildup, thus reducing queuing delays and minimizing latency.

Table 1 below shows ECN threshold and marking probability values for throughput-first and latency-first modes.

Table 1. ECN Threshold and Marking Probability: Throughput-First vs. Latency-First

Easy ECN Mode	ECN Threshold and Marking Probability	Tomahawk3	Trident3-X5/Trident3-X7	Tomahawk5
throughput-first	min_thresh (Bytes)	5,080,000	2,560,000	2,540,000
	max_thresh (Bytes)	25,400,000	12,800,000	12,700,000
	drop_probability	20%	20%	20%
latency-first	min_thresh (Bytes)	508,000	256,000	254,000
	max_thresh (Bytes)	2,540,000	1,280,000	1,270,000

	drop_probability	20%	20%	20%

To simplify the configuration, users can enable Easy ECN for global congestion management. However, if the global configuration does not fully address the specific needs of queue-level congestion management, standard ECN can be fine-tuned for individual interface queues.

> **NOTE**:
>
> When both global configuration and user-specified interface queue settings are applied, the settings for the user-specified interface queue will take effect.

Configuration Notes and Constraints

When configuring Easy ECN, consider the following points:

- Easy ECN is only supported on **Trident3-X5**, **Trident3-X7**, **Tomahawk3** and **Tomahawk5** platforms.
- **Throughput-First** mode prioritizes high data transfer rates. It is ideal for environments where bulk data transmission is critical. **Latency-First** mode focuses on minimizing delays in packet transmission, making it suitable for real-time applications (e.g., VoIP, video streaming).
- Easy ECN provides a simplified, global configuration for congestion management. If more granular control is required, standard ECN can be configured on specific interface queues. In such cases, interface-specific ECN configurations override global settings.

Configuring Easy ECN

To simplify the configuration, users can enable Easy ECN for global congestion management. However, if the global configuration does not fully address the specific needs of queue-level congestion management, standard ECN can be fine-tuned for individual interface queues.

The following command can be used to enable easy ECN globally.

set class-of-service easy-ecn mode <**throughput-first** | **latency-first**>

Example

- Configure easy ECN mode to **latency-first**.

```
admin@PICOS# set class-of-service easy-ecn mode latency-first
admin@PICOS# commit
```

- Configure easy ECN mode to **throughput-first**.

```
admin@PICOS# set class-of-service easy-ecn mode throughput-first
admin@PICOS# commit
```

PFC and ECN Statistical Reporting through gRPC

In modern network systems, efficient congestion management and data flow control are crucial to maintain high-performance levels, especially in data centers and cloud environments. PFC (Priority Flow Control) and ECN (Explicit Congestion Notification) are two complementary mechanisms that help manage traffic and congestion, while **gRPC** (Google Remote Procedure Call) facilitates real-time communication and reporting between network components.

PFC and ECN work together to handle congestion in a network. PFC ensures that critical traffic continues to flow by pausing lower-priority traffic, while ECN marks packets to indicate congestion. This cooperation minimizes packet loss and optimizes network performance.

As PFC and ECN manage traffic, they generate valuable statistics such as the number of paused frames (PFC) and the number of ECN-marked packets. These statistics are essential for understanding network health and congestion levels.

gRPC is used to gather and transmit these statistics to a central server. Because gRPC is designed for high-performance, low-latency communication, it is well-suited to handle the real-time transmission of PFC and ECN data. The statistical data can be analyzed to adjust network policies, improve performance, and prevent future congestion.

PFC and ECN Statistics

PFC and ECN, in conjunction with gRPC, can provide PFC pause frame counts, PFC deadlock monitoring and ECN-marked packet counts for statistical queries.

The statistics that PFC supports reporting include:

- Number of PFC pause frames sent
- Number of PFC pause frames received
- Number of PFC deadlock monitoring instances
- Number of PFC deadlock recovery instances
- Rate of PFC pause frames received
- Rate of PFC pause frames sent

The statistics that ECN supports reporting include:

- Number of ECN marked packets
- Rate of ECN marked packets

Configuration Procedure

1. Configure PFC on your network devices. Refer to Configuring Priority-based Flow Control (PFC) for details about how to configure PFC.
2. Enable ECN to help manage congestion. Refer to Configuring Explicit Congestion Notification (ECN) for details about how to enable ECN.
3. Deploy gRPC servers and clients to handle the statistical query requests. Refer to Configuring gNMI-gRPC Based Telemetry Technology for details about how to deploy gRPC.

This setup ensures you have real-time monitoring and statistical analysis capabilities for PFC and ECN, which can significantly aid in preventing network performance issues due to congestion and deadlocks.

Configuring Dynamic Load Balancing

- Overview
- Implementation Principle
  - Normal Mode
  - Optimal Mode
  - Assigned Mode
- Restrictions and Guidelines
- Configuring Dynamic Load Balancing
  - Procedure
  - Configuration Example
  - Verify the Configuration

Overview

Traditional static load balancing does not consider the utilization of each member link within the load-balancing group, leading to uneven load distribution among the member links. This issue becomes more pronounced with the appearance of large data flows, exacerbating congestion on the selected member link and potentially causing packet loss.

By enabling dynamic load balancing, the traffic of Equal-Cost Multi-Path (ECMP) routing can be distributed across different member links through dynamic load balancing, maximizing load balancing among the member links.

Implementation Principle

PICOS supports three modes of Dynamic load balancing: **Normal Mode**, **Optimal Mode** and **Assigned Mode**.

Normal Mode

There is link transmission delay between two directly connected devices. If the time interval between two data packets to be sent is greater than the maximum link transmission delay of the member links in the load-balancing group, these two packets can be forwarded using different member links without causing out-of-order delivery at the receiving end. Normal mode dynamic load balancing is based on this principle.

In Normal mode, the device determines the time interval between the packet to be forwarded and the previous packet in its flow. If the interval is greater than the maximum link transmission delay of the member links, the packet to be forwarded is considered the first packet of a new flowset. If the interval is less than the maximum link transmission delay, the packet is considered part of the same flowset as the previous packet.

The device forwards the packets based on the flowset, selecting the member link with the lighter load for forwarding. Packets within the same flowset are forwarded using the same member link.

Optimal Mode

The Optimal mode of dynamic load balancing operates on a per-packet distribution system, where each packet is forwarded independently based on the real-time load conditions of the available links. This mechanism allows the device to select the least congested or lightly loaded link at any given moment, distributing the packets dynamically to optimize network performance. However, this method introduces a potential issue when packets belonging to the same flow are forwarded through different links. If the time interval between two consecutively sent packets is shorter than the maximum transmission delay across the links, the packets may arrive out of order at the receiving end. This happens because different links may have varying transmission delays, causing later-sent packets to arrive before earlier ones.

For this reason, Optimal mode can lead to out-of-order packet delivery, particularly in scenarios where flows are split across multiple paths. Out-of-order packets can disrupt certain types of network traffic, especially those that rely on sequence consistency, such as real-time voice or video communication. To mitigate this, it is crucial that the receiving device or terminal has the capability to reorder packets properly. Devices must be equipped with reassembly buffers or out-of-order packet handling mechanisms to ensure the integrity of the flow, allowing the receiving system to reorder the packets correctly before processing them. Optimal mode, while improving load distribution and avoiding bottlenecks, requires robust support on the receiving end to handle these potential sequencing issues effectively.

Assigned Mode

In Assigned mode dynamic load balancing, the system ensures that each packet within a specific flow follows a consistent path by using the same forwarding link as the previous packet in that flow. This approach minimizes the risk of out-of-order packet delivery by keeping the traffic for the flow on the same route. However, when a flow starts and the first packet is sent, the system cannot rely on a previous packet's path. In this case, a static load balancing mechanism comes into play, where a hash-based algorithm determines the member link to forward the packet. The hash function typically considers factors such as source and destination IP addresses or port numbers to ensure an even distribution of traffic across the available links while maintaining flow consistency. Once the path is set for the first packet, subsequent packets in the same flow will continue to follow that route until the flow is completed.

Restrictions and Guidelines

When you configure Dynamic Load Balancing, follow these restrictions and guidelines:

- Dynamic Load Balancing for ECMP is only supported on **Trident3**, **Tomahawk3** and **Tomahawk5** platforms.
- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-optimal**, **dlb-assigned** and **dlb-normal**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Configuring Dynamic Load Balancing

Procedure

Step 1 Enable one of the three modes of Dynamic load balancing for ECMP: **Normal mode**, **Optimal mode** and **Assigned mode**.

set interface ecmp hash-mapping dlb-normal [**flowset-time** <*flowset-time*>]

set interface ecmp hash-mapping dlb-optimal

set interface ecmp hash-mapping dlb-assigned

By default, Dynamic Load Balancing for ECMP is disabled.

Step 2 Commit the configuration.

commit

Step 3 Under CLI operational mode (prompted with ">"), run the following command to restart the system for the configuration to take effect.

request system reboot

Configuration Example

- The following commands enable normal mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
```

```
admin@PICOS# exit
admin@PICOS> request system reboot
```

- The following commands change Dynamic Load Balancing normal mode to optimal mode for ECMP.

```
admin@PICOS# delete interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
admin@PICOS# set interface ecmp hash-mapping dlb-optimal
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

Verify the Configuration

- Use the command **run show route ipv4** to view the ECMP routes. In the following show result, we can see that the destination address 10.20.51.0/24 is reached via three different next hops: 192.168.0.1, 192.168.1.1, and 192.168.2.1, forming ECMP routes.

```
admin@PICOS# run show route ipv4
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, T - Table, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

K * 0.0.0.0/0 [255/8192] unreachable (blackhole), 23:42:36
K>* 0.0.0.0/0 [0/2] via 10.10.51.1, eth0, 23:42:36
C>* 10.10.51.0/24 is directly connected, eth0, 23:42:36
S>* 10.20.51.0/24 [1/0] via 192.168.0.1, vlan10, weight 1, 00:09:06
  *                     via 192.168.1.1, vlan20, weight 1, 00:09:06
  *                     via 192.168.2.1, vlan30, weight 1, 00:09:06
C>* 192.168.0.0/24 is directly connected, vlan10, 00:09:09
C>* 192.168.1.0/24 is directly connected, vlan20, 00:09:09
C>* 192.168.2.0/24 is directly connected, vlan30, 00:09:09
```

- Use the command **run show interface gigabit-ethernet** <*interface-name*> to view the traffic distribution for each interface. Here is an example:

```
admin@PICOS# run show interface gigabit-ethernet ge-1/1/5
Physical interface: ge-1/1/5, Enabled, error-discard False, Physical link is Up
Interface index: 5, Mac Learning Enabled
Port mode: trunk
Description:
Link-level type: Ethernet, MTU: 1518, Speed: 2.5Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Enabled, Advertised speed modes: 10M,100M,1G,2.5G
Interface flags: SNMP-Traps Internal: 0x0
Interface rate limit  ingress: unlimited, egress: unlimited
Interface burst limit ingress: unlimited, egress: unlimited
Precision Time Protocol mode: none
Current address: 1c:72:1d:c9:1b:e1, Hardware address: 1c:72:1d:c9:1b:e1
Traffic statistics:
  5 sec input rate 5440 bits/sec, 1 packets/sec
  5 sec output rate 0 bits/sec, 0 packets/sec
  Input Packets.....................12235
  Output Packets.....................135
  Input Octets.....................3943964
  Output Octets.....................14660
```

Typical Configuration Example of Lossless Network

Networking Requirements

Procedure

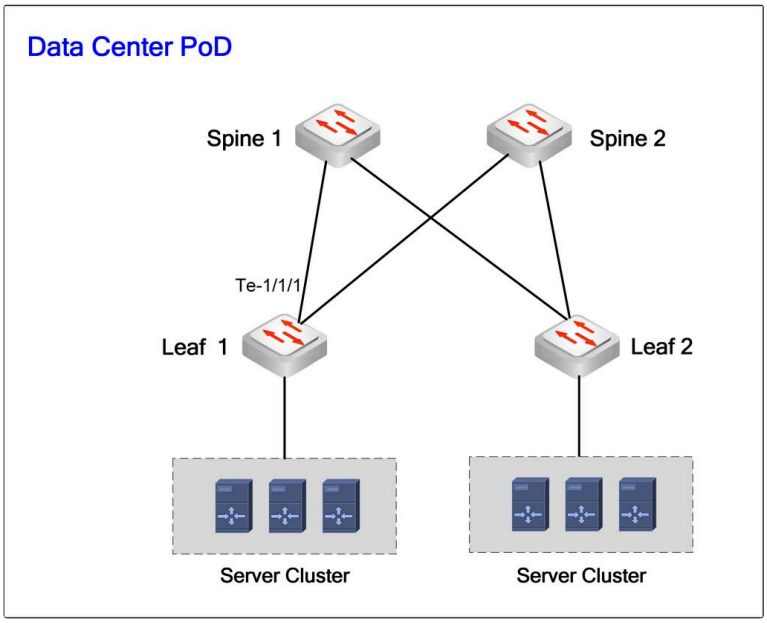
Networking Requirements

In **Figure 1**, in the following data center network PoD, two Server Clusters are connected to the network through devices Leaf 1, Leaf 2, Spine 1 and Spine 2. A lossless network is required to apply in the network devices to prevent packet loss during data transmission, ensuring high reliability and performance, especially for applications that are sensitive to latency and data integrity.

Setting up a lossless network involves careful planning, consistent configuration across all devices, and continuous monitoring and management. Follow the configuration roadmap below to ensure all components are correctly configured:

- Configure **PFC** on all relevant ports to prevent packet loss by pausing traffic during congestion.
- Employ a **PFC watchdog** mechanism to detect and mitigate PFC deadlocks.
- Enable Explicit Congestion Notification (ECN) on all switches and endpoints to signal congestion without dropping packets. Configure ECN thresholds to detect and mark packets early before severe congestion occurs.
- Enable dynamic load balancing, the traffic of Equal-Cost Multi-Path (ECMP) routing can be distributed across different member links through dynamic load balancing.

Figure 1. Typical Configuration Example of Lossless Network



Procedure

The following configuration steps are for Leaf 1. The configurations for Leaf 2, Spine 1 and Spine 2 are similar to Leaf 1 and will not be repeated.

Step 1 On Leaf 1, configure **PFC** on all relevant ports to prevent packet loss by pausing traffic during congestion.

The following commands complete the configurations:

- Configure PFC profile `pfc1`.
- Apply PFC profile to the port `te-1/1/1`.

```
admin@PICOS# set class-of-service pfc-profile pfc1
admin@PICOS#set class-of-service interface te-1/1/1 pfc-profile pfc1
admin@PICOS# commit
```

- Show the class of service statistics information on specified interface.

The class 0~7 in PFC frame corresponds to the following "802.1P" item. The value of ”RxPFC“ item will be incremented by 1 if te-1/1/1 receives a PFC frame. The value of ”TxPFC“ item will be incremented by 1 if te-1/1/1 sends out a PFC frame.

```
admin@PICOS# run show class-of-service interface te-1/1/1
Interface : te-1/1/1
802.1P         Priority Flow Control    RxPFC              TxPFC
-----------    ---------------------    ---------------    ---------------
0              true                     0                  500
1              true                     0                  0
2              true                     0                  71
3              true                     0                  0
4              true                     0                  0
5              true                    0                  0
6              true                     0                  102
7              true                     0                  0
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule               Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

Step 2 (Optional) Configure the PFC buffer.

After the PFC function is enabled, the default storage space is available for priority queues. You can flexibly make good use of the storage space through configuring buffer thresholds based on certain queues as needed.

The following commands complete the configurations:

- Set the upper threshold of guaranteed buffer for PFC queue 3 on the ingress interface te-1/1/1 as 24000 cells.
- Set the static threshold of shared buffer for PFC queue 1 on the ingress interface te-1/1/1 as 10000 cells.
- Set the offset value of shared buffer for PFC queue 1 on the ingress interface te-1/1/1 as 3000 cells.

```
admin@PICOS# set interface gigabit-ethernet te-1/1/1 ethernet-switching-options buffer ingress-queue 3
guaranteed 24000
admin@PICOS# set interface gigabit-ethernet te-1/1/1 ethernet-switching-options buffer ingress-queue 1
threshold 10000
admin@PICOS# set interface gigabit-ethernet te-1/1/1 ethernet-switching-options buffer ingress-queue 1 reset-
offset 3000
admin@PICOS# commit
```

Step 3 Configure PFC watchdog.

The following commands complete the configurations:

- Enable PFC watchdog on queue5 of interface te-1/1/1.

- Configure the time interval of PFC deadlock detection to 10 x 100ms, where 100ms is the default value of PFC deadlock detection timer granularity.
- Configure the restore time to 10 x 100ms when PFC deadlock occurs, where 100ms is the default value of PFC deadlock restore timer granularity.

```
admin@PICOS# set class-of-service interface te-1/1/1 pfc-watchdog code-point 5 enable true
admin@PICOS# set class-of-service pfc-watchdog code-point 5 detect-interval 10
admin@PICOS# set class-of-service pfc-watchdog code-point 5 restore-interval 10
admin@PICOS# commit
```

After the configuration, use command **run show pfc-watchdog config** to view the configuration information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog config
      PORT         ACTION          QUEUE    DETECTION TIME    RESTORATION TIME
----------    -----------   ------------  ----------------  ------------------
te-1/1/1          forward            5              1000                1000
```

Use command **run show pfc-watchdog stats** to view the statistics information about PFC watchdog, including the number of PFC pause storms that have been detected and restored, as well as the number of packets that have been dropped, on the PFC queues on an interface.

```
admin@PICOS# run show pfc-watchdog stats
       QUEUE       STATUS    STORM DETECTED/RESTORED        TX OK/DROP    TX LAST OK/DROP
------------  -----------  -------------------------  ----------------  -----------------
te-1/1/1:5       stormed                      9/8      82072626556/0      32053822365/0
```

Step 4 Configure ECN.

Users have to continuously monitor network performance and ECN marking rates. Make dynamic adjustments to the ECN thresholds as needed to respond to changing network conditions.

The following commands complete the configurations:

- Enable WRED on queue 0 of interface te-1/1/1;
- Set the maximum threshold to 400 and the minimum threshold to 200 on queue 0 of interface te-1/1/1;
- Set the drop probability to 50% on queue 0 of interface te-1/1/1;
- Enable ECN (Explicit Congestion Notification) on queue 0 of interface te-1/1/1.

```
admin@PICOS# set interface gigabit-ethernet te-1/1/3 wred queue 0 enable true
admin@PICOS# set interface gigabit-ethernet te-1/1/3 wred queue 0 max_thresh 400
admin@PICOS# set interface gigabit-ethernet te-1/1/3 wred queue 0 min_thresh 200
admin@PICOS# set interface gigabit-ethernet te-1/1/3 wred queue 0 drop_probability 50
admin@PICOS# set interface gigabit-ethernet te-1/1/3 wred queue 0 ecn_thresh 1
admin@PICOS# commit
```

Show the WRED information of the specified interface.

```
admin@PICOS# run show interface gigabit-ethernet te-1/1/1 wred
Queue Num    Min Thresh   Max Thresh   Drop Probability    ECN Thresh      Status
----------   ----------   ----------   ----------------    -----------     ----------
0              200            400            50%             Enabled        Enabled
1              0              0              0%              Disabled       Disabled
2              0              0              0%              Disabled       Disabled
3              0              0              0%              Disabled       Disabled
4              0              0              0%              Disabled       Disabled
5              0              0              0%              Disabled       Disabled
6              0              0              0%              Disabled       Disabled
7              0              0              0%              Disabled       Disabled
```

Step 5 Enable normal mode of Dynamic Load Balancing for ECMP.

By enabling dynamic load balancing, the traffic of Equal-Cost Multi-Path (ECMP) routing can be distributed across different member links through dynamic load balancing, maximizing load balancing among the member links.

```
admin@PICOS# set interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
```

OpenFlow in Crossflow Mode

- Crossflow Mode Introduction
- CrossFlow Mode Known Limitations
- Crossflow Basic Configuration
- Configuration Example1 in Crossflow Mode
- Configuration Example2 in Crossflow Mode
- Example for Configuring STM Resource Allocation
- Multi-action in crossflow mode

Crossflow Mode Introduction

This chapter describes the details of OpenFlow via CrossFlow mode. CrossFlow mode allows traditional L2/L3 and OpenFlow protocols to run simultaneously on the same physical switch.

Warning:
On FS S5810 Series and S5860 Series switches, run "save_config" command when set Crossflow commands. Otherwise, the Crossflow configuration will be lost after PicOS reboot. For detail, please refer to Configuration Saving Guide.

CrossFlow mode has been greatly improved starting in PicOS 2.6.2. Now, most of the OVS mode commands are available in CrossFlow mode.

OVS features that are available in the CrossFlow mode:

- controller (test ok)
- egress-mode (test ok)
- combinated-mode (test ok)
- multi-table (test ok)
- max-ecmp-ports (test ok)
- loopback-enable (test ok)
- flow-counter-mode (test ok)
- GRE (test ok)
- meter (test ok)
- group (test ok)
- Q-in-Q (test ok)
- udf-mode(test ok)
- manager(test ok)
- mpls flow entries(test ok)

OVS features that need to be configured in Xorplus mode:

- qos (test ok)
- qe-port-mode (test ok)
- lag-advance-hash-mapping-fields (test ok)
- LACP (test ok)

The OVS features which are unavailable in CrossFlow mode:

- proxy-arp
- proxy-icmpv6
- pbb flow entries
- VxLAN
- L2MPLS
- L2GRE
- match-mode

Configuration Notes:

- Only Openflow ports can be added to an Openflow lag as members, and only Crossflow ports can be added to a Crossflow lag as members. All lag's members are configured in Switching CLI.
- All LACP packets are handled by Switching.
- Besides LACP, all other protocol packets received from Openflow ports will be sent to OVS. For the packets received from Crossflow ports, user can configure either Switching or OVS to handle the packets. By default, these packets are handled by Switching.
- All port speed, mtu, VLAN members, and other information is configured in Switching CLI as usual, and these configurations in OVS CLI will not take effect.
- When add flow with matching mpls,mpls_label cannot be configured as 0-15.

The Switch Hardware Architecture page describes the meaning of some terms used here, such as TCAM or FIB.

CrossFlow Mode Introduction

In CrossFlow mode, switches can achieve most of the functions that exist in OVS mode, including: basic flow function, meter, group, multi-table, Q-in Q and so on.

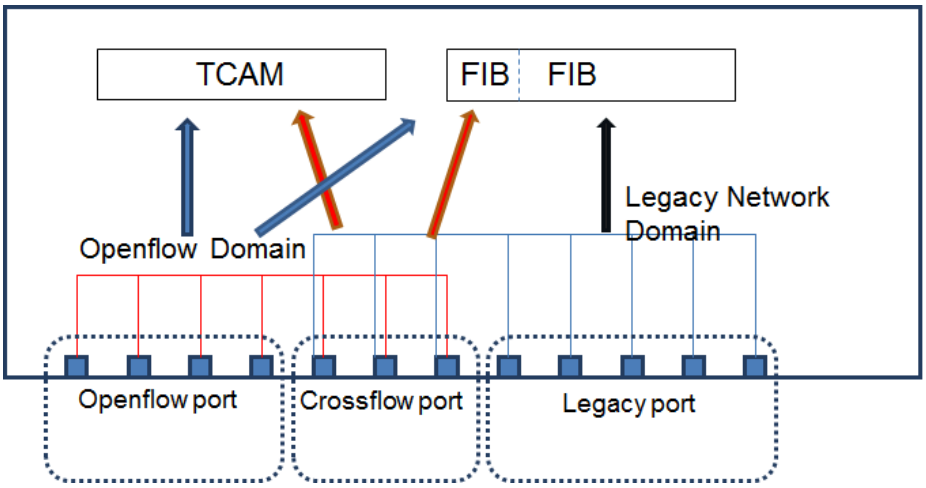
- Like in PicOS OVS mode, in CrossFlow mode, OpenFlow 1.0, OpenFlow 1.1, OpenFlow 1.2, OpenFlow 1.3, and OpenFlow 1.4 are supported. User can configure any supported version in the CLI.
- After PicOS 2.6.2, ports in the switch can be configured in any one of these three modes: Legacy, Crossflow or Openflow. The difference in configuration is:

  Legacy port: disable crossflow

  Crossflow port: enable crossflow and enable local-control

  Openflow port: enable crossflow and disable local-control

- After PicOS 2.4, Openflow can also support the multiple-table control, which means that Openflow can configure some flows in FIB (mac address table and routing table). The flow should match some conditions to install them in FIB. Please refer to the manual in the PicOS Openflow Configuration documentation.



As the figure above shows, the switch ports working status in Crossflow mode is shown. The Openflow flow can look up two tables including TCAM and FIB (multiple tables). The ports in Crossflow mode can be summarized as follows:

Enable Crossflow mode and local-control disable (Openflow port):

1. The port is completely controlled by Openflow
2. All broadcast turned off and auto learning turned off
3. Packet forwarded by looking up the TCAM table default
4. Packet forwarded by looking up the FIB once enable multi-table and configure L2/L3 flow table

Enable Crossflow mode and local-control enable (Crossflow port):

1. The port is controlled by both local legacy stack and Openflow.
2. All broadcast is turned on and auto learning is turned on
3. Packet is forwarded by looking up the FIB (FDB/routing table) and TCAM table
4. No matter if multi-table is enabled or not, packets all can forward by looking up the FIB

Disable Crossflow mode (Legacy port):

1. The port is controlled by local legacy stacks.
2. All broadcast is turned on and auto learning is turned on.
3. Packet is forwarded by looking up the FIB (FDB/routing table).

In Crossflow mode, user can enable L2/L3 mode as a PicOS OVS multi-table function. If the L2/L3 mode is enabled, the FIB table resource will be shared by legacy ports and Crossflow ports, and data traffic cannot mix between the different type ports. User can allocate the resource for special ports as the following command shows.

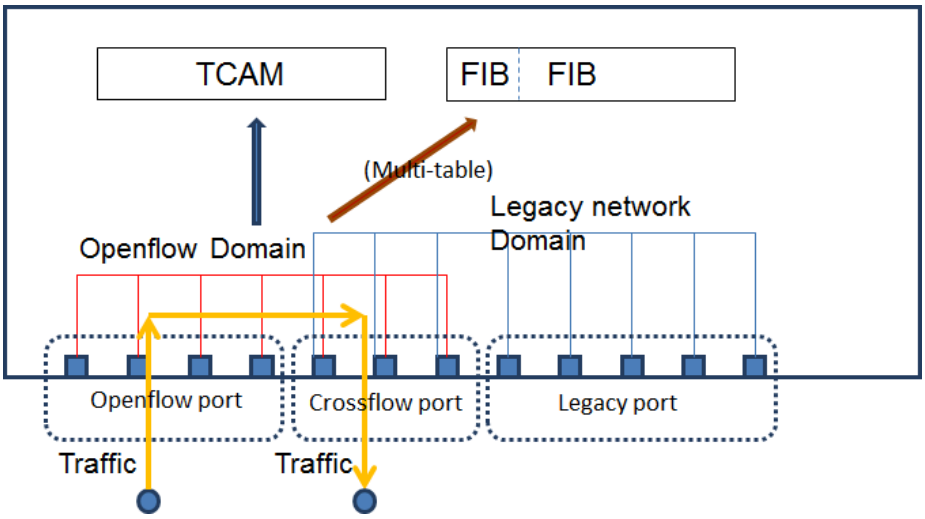
```
set interface stm firewall-table ingress 100
set interface stm mac-table 20000
set interface stm ipv4-route 6000
set interface stm ipv6-route 1000
```

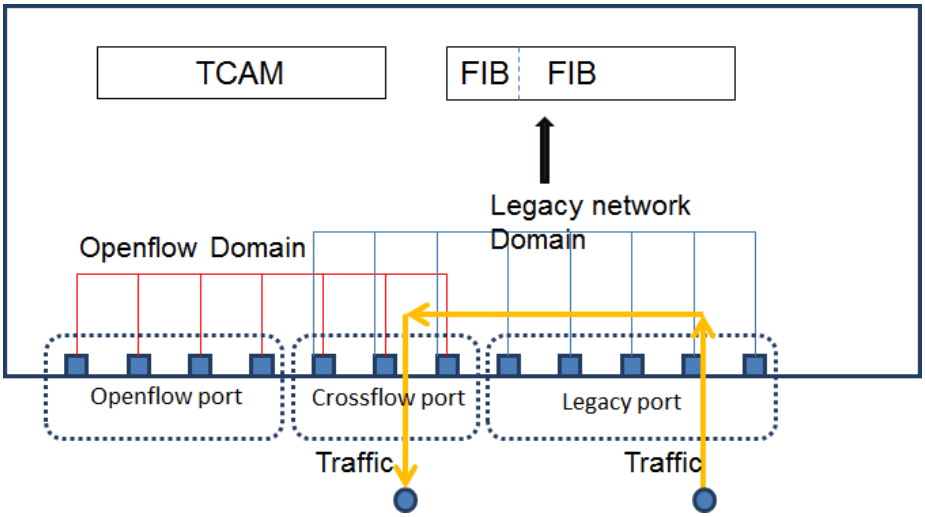
The first command, **set interface stm firewall-table ingress 100**, means allocate the TCAM resource for ingress ACL rule, and part of the rest of resource for Crossflow port and Openflow port;

The second command, **set interface stm mac-table 20000**, means allocate the FDB table resource for legacy port, and the rest of resource for Crossflow port and Openflow port.

The last two commands, **set interface stm ipv4-route 6000,** and **set interface stm ipv6-route 1000**, means allocate the route table resource for legacy port, and the rest of resources for Crossflow port and Openflow port.

In Crossflow mode, traffic can only be forwarded in the OpenFlow or Legacy network domain (as shown in the following figures). The traffic between Openflow port and Crossflow port forwarded by Tcam flow table default, if user wants to forward by FIB, enable multi-table and configure L2/L3 flow entries. The traffic between Crossflow port and Legacy port is forwarded by FIB.





Install a flow with action "NORMAL":

1. By default, the traffic output port will be replaced by the TCAM flow's action after packets are switched and routed. e.g. A packet matches a route and decides the output port (ge-1/1/10) by a route, then it also matches a TCAM flow which has the output port ge-1/1/12, Then, the packet will be forwarded to ge-1/1/12 because the TCAM flow action will replace the original route output port.
2. When a flow in TCAM has an action "NORMAL", the packet which has decided the output port after route table, will still be forwarded to route output port. "NORMAL" means there is no change to the packet output port.
3. When a route packet will not match any flows in TCAM, the output port also will not be changed.

CrossFlow Mode Known Limitations

Conflict Management between OpenFlow and CLI Configurations

The physical configurations of the FDB table and routing table of Openflow should not conflict with the CLI configurations. This means that Openflow can install a flow in the routing table at the same time that legacy network installs a flow in routing table without conflicts. If these configurations conflict, the later configuration will fail.

set firewall filter description and OpenFlow TCAM Flows may conflict. For instance, the OpenFlow rule could be dropping a specific type of packet when the Firewall filters are forwarding them. In this case, both rules are performed concurrently and independently, and the results of the matches are merged. When there are no conflicting results, all results are applied. When there are overlapping and conflicting results, the conflicted parts of the result are selected based on priorities. DROP action has the highest priority, followed by REDIRECT, REPLACE, and TCAM slice number. (OpenFlow rules and Firewall rules are places in different TCAM Slices.)

In CrossFlow mode, the ACL filter has a higher priority than that of Openflow flow entry.

Because arp works in different group with ip,so if there is one or more openflow ports, the arp packets will be dropped because drop actions has the highest priority.And you can add a flow like this:ovs-ofctl add-flow br0 priority=1,actions=normal

Default Drop In OpenFlow

There is a default drop flow in the system when user enables Crossflow mode, and this drop flow only applies to the Openflow ports.

Other Limitations

From PicOS-2.6, some ports can work within both the legacy network domain and the Openflow domain. We call these ports Crossflow ports.

If user enables multi-table and configures L2/L3 flow entry on the Openflow port, traffic from the legacy port can also match the L2/L3 flow entry and be forward on the Openflow port.

If packets can match TCAM flow entry and route table at the same time, the TCAM flow entry has the higher priority. Because the packets must go through FIB table, if there is no mod-src-mac in the TCAM flow entry, the packets will be modified by the src-mac in FIB table then go out as a TCAM flow entry.

If a packet needs match to a Crossflow port, it must have in_port in match field when adding flow.

Crossflow Basic Configuration

OpenFlow is supported in PicOS, and user can configure PicOS switches with both legacy network protocol and Openflow, which will provide extreme flexibility in network deployment.

Configure ovsdb-server Locally

Check the ovsdb-server state on the switch. By default, the ovsdb-server listens to the local switch, and the ovs-vswitchd can only be configured by the local switch.

```
admin@XorPlus$ps aux|grep ovs
root      5174  0.5  0.7  46716  3900 ?        S<l  01:41   0:07 /xorplus/bin/system/tools/xorplus_monitor -c 80 -r
root      5205  0.0  0.1   6288   624 ?        Ss   01:42   0:00 ovsdb-server: monitoring pid 5206 (healthy)
root      5206  0.0  0.4   6432  2124 ?        S    01:42   0:00 /ovs/sbin/ovsdb-server --pidfile --log-file --deta
root      5208  0.0  1.0  49580  5388 ?        Sl   01:42   0:00 /ovs/sbin/ovs-vswitchd --enable-shared-lcmgr
admin     5219  0.0  0.1   2128   684 ttyS0    S+   02:01   0:00 grep --color=auto ovs
```

Configure ovs-vswitchd Locally

```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@XorPlus$ovs-vsctl add-port br0 ge-1/1/21 -- set interface ge-1/1/21 type=pica8
admin@XorPlus$ovs-vsctl set-controller br0 tcp:10.10.51.59:6633
```

Configure ovsdb-server Remotely

Modify the ovsdb-server state on the switch. Configure the ovsdb-server listening switch management-ethernet interface IP 10.10.51.138 and PORT 6640.

```
admin@XorPlus$ps aux|grep ovs
root      5174  0.6  0.7  46716  3900 ?        S<l  01:41   0:10 /xorplus/bin/system/tools/xorplus_monitor -c 80 -r
root      5205  0.0  0.1   6288   624 ?        Ss   01:42   0:00 ovsdb-server: monitoring pid 5206 (healthy)
root      5206  0.0  0.4   6432  2136 ?        S    01:42   0:00 /ovs/sbin/ovsdb-server --pidfile --log-file --deta
root      5208  0.3  1.2  75456  6520 ?        Sl   01:42   0:05 /ovs/sbin/ovs-vswitchd --enable-shared-lcmgr
admin     5262  0.0  0.1   2128   684 ttyS0    S+   02:09   0:00 grep --color=auto ovs
admin@XorPlus$
admin@XorPlus$sudo kill -9 5206
admin@XorPlus$
admin@XorPlus$sudo /ovs/sbin/ovsdb-server --pidfile --log-file --detach --monit
or --remote=ptcp:6640:10.10.51.144 --remote=punix:/ovs/var/run/openvswitch/db.s
ock --remote=db:Open_vSwitch,Manager,target --private-key=db:hardware_vtep,SSL,
private_key --certificate=db:hardware_vtep,SSL,certificate --bootstrap-ca-cert=
db:hardware_vtep,SSL,ca_cert /ovs/ovs-vswitchd.conf.db /xorplus/config/vtep.db
2002-06-25T02:15:31Z|00001|vlog|INFO|opened log file /ovs/var/log/openvswitch/ovsdb-server.log
admin@XorPlus$
admin@XorPlus$ps aux|grep ovs
root      5174  0.5  0.7  46716  3900 ?        S<l  01:41   0:12 /xorplus/bin/system/tools/xorplus_monitor -c 80 -r
root      5208  0.2  1.2  75456  6520 ?        Sl   01:42   0:05 /ovs/sbin/ovs-vswitchd --enable-shared-lcmgr
root      5267  0.0  0.1   6288   628 ?        Ss   02:15   0:00 ovsdb-server: monitoring pid 5268 (healthy)
root      5268  0.5  0.4   6432  2124 ?        S    02:15   0:00 /ovs/sbin/ovsdb-server --pidfile --log-file --deta
admin     5270  0.0  0.1   2128   684 ttyS0    S+   02:15   0:00 grep --color=auto ovs
admin@XorPlus$
```

Configure ovs-vswitchd by Remote Server 10.10.50.42

```
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.144:6640 add-br br0 -- set bridge br0 datapath_type=pica8
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.144:6640 add-port br0 ge-1/1/21 -- set interface ge-1/1/21 type=pica8
root@dev-42:~# ovs-vsctl --db=tcp:10.10.51.144:6640 set-controller br0 tcp:10.10.51.59:6633
```

Configuration Example1 in Crossflow Mode

Configure the OpenFlow Port in CrossFlow Mode

Commands:

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 crossflow local-control false
admin@XorPlus# set vlans vlan-id 2,2000,4094
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 2000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members 4094
admin@XorPlus# commit
```

Commands in Linux:

```
admin@XorPlus$ovs-vsctl list pica8
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@XorPlus$ovs-vsctl add-port br0 ge-1/1/1 -- set Interface ge-1/1/1 type=pica8
```

Configure the Hybrid Port in CrossFlow Mode

Commands:

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 crossflow enable true
admin@XorPlus# set vlans vlan-id 2,2000,4094
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 2
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 2000
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching vlan members 4094
admin@XorPlus# commit
```

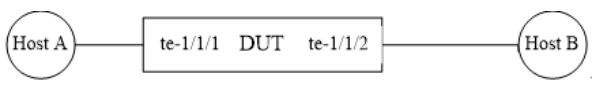
Commands in Linux:

```
admin@XorPlus$ovs-vsctl list pica8
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
admin@XorPlus$ovs-vsctl add-port br0 ge-1/1/2 -- set Interface ge-1/1/2 type=crossflow
```

Examples

Basic Configurations

topology



Step 1: Configure port te-1/1/1 as OpenFlow port and te-1/1/2 as CrossFlow port

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
```

```
admin@XorPlus# set vlans vlan-id 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 2,10,20
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 speed 1000
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 speed 1000
admin@XorPlus# commit
```

Step 2: Exit the Xorplus system, then enter Linux system

```
admin@XorPlus#exit
admin@XorPlus>exit
admin@XorPlus$
```

Step 3: Create a new bridge named br0

```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 4: Add ports to br0

```
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/1 -- set Interface te-1/1/1 type=pica8
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/2 -- set Interface te-1/1/2 type=crossflow
```

Step 5: Add a flow

```
admin@XorPlus$ovs-ofctl  add-flow br0 in_port=1,actions=output:2
```

Step 6: Send packets to te-1/1/1

Send untagged packets to te-1/1/1 that match this flow. Then, te-1/1/2 will forward the packets (with no vlan). Send packets with vlan 2 to te-1/1/1. Then, te-1/1/2 will forward the packets (with vlan 2).

Lag Configurations

Step 1: Set lag interface (Only Openflow ports can be added to an openflow lag as members, and only Crossflow ports can be added to a Crossflow lag as members.)

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@XorPlus# commit
admin@XorPlus#set interface aggregate-ethernet ae1 crossflow enable true
admin@XorPlus#set interface aggregate-ethernet ae1 crossflow local-control false
admin@XorPlus#set interface aggregate-ethernet ae2 crossflow enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 speed 1000
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 speed 1000
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad ae1
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad ae2
admin@XorPlus# commit
admin@XorPlus#set vlans vlan-id 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 2,10,20
admin@XorPlus# set interface aggregate-ethernet ae2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae2 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
```

Step 2: Exit the Xorplus system, then enter Linux system

```
admin@XorPlus#exit
admin@XorPlus>exit
```

```
admin@XorPlus$
```

Step 3: Create a new bridge named br0.

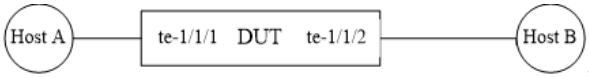
```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 4: Add ports to br0.

```
admin@XorPlus$ovs-vsctl add-port br0 ae1 -- set Interface ae1 type=pica8_lag
admin@XorPlus$ovs-vsctl add-port br0 ae2 -- set Interface ae2 type=pica8_lag
```

Flow Priority Configurations

topology



Step 1: Configure two ports as Openflow ports

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow local-control false
admin@XorPlus# set vlans vlan-id 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
```

Step 2: Exit the Xorplus system, then enter Linux system

```
admin@XorPlus#exit
admin@XorPlus>exit
admin@XorPlus$
```

Step 3: Create a new bridge named br0.

```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 4: Add ports to br0.

```
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/1 -- set Interface te-1/1/1 type=pica8
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/2 -- set Interface te-1/1/2 type=pica8
```

Step 5: Add two flows

```
admin@XorPlus$ovs-ofctl  add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=output:2
admin@XorPlus$ovs-ofctl  add-flow br0 in_port=1,priority=50000,dl_src=22:11:11:11:11:11,actions=mod_dl_src:22:22:2
```

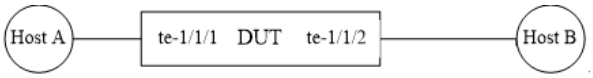
Step 6: Send packets to te-1/1/1

Send untagged packets to te-1/1/1 that match this flow, then te-1/1/2 will forward the packets (with no vlan), and the packets' source mac address is modified to 22:22:22:22:22:22, because the priority of the second flow is higher than that of the first flow.

Send packets with vlan 2 to te-1/1/1, then te-1/1/2 will forward the packets with vlan 2 and the packets' source mac address is modified to 22:22:22:22:22:22.

FDB Configurations

topology



Step 1: Configure two ports as Openflow ports

Step 2: Exit the Xorplus system, then enter Linux system

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow local-control false
admin@XorPlus#set vlans vlan-id 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
admin@XorPlus#exit
admin@XorPlus>exit
admin@XorPlus$
```

Step 3: Create a new bridge named br0.

```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 4: Add ports to br0.

```
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/1 -- set Interface te-1/1/1 type=pica8
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/2 -- set Interface te-1/1/2 type=pica8
```

Step 5: Set table 1 to FDB table

```
admin@XorPlus$ovs-vsctl set-l2-mode true 1
```

Step 6: Add a flow

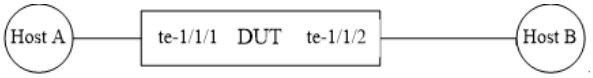
```
admin@XorPlus$ovs-ofctl  add-flow br0 table=1,dl_dst=22:22:22:22:22:22,dl_vlan=10,actions=output:2
```

Flows must match dl_dst,dl_vlan and output port if they want to be stored in FDB table. Table number of FDB table is 251 by default. User can specify another table as the FDB table instead of the 251 by using this command: ***ovs-vsctl set-l2-mode true [table number].***

If you want flows to be stored in ROUTE table, flows must match dl_dst,dl_vlan,dl_type,nw_dst, and mod_dl_dst in action, and the default table number of ROUTE is 252. Use command ***ovs-vsctl set-l3-mode true [table number]*** to set route table.

Route Configurations

topology



Step 1: Configure two ports as Openflow ports

Step 2: Exit the Xorplus system, then enter Linux system

```
admin@XorPlus# set xovs enable true
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow local-control false
admin@XorPlus#set vlans vlan-id 2,10,20
admin@XorPlus# commit
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
```

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching vlan members 2,10,20
admin@XorPlus# commit
admin@XorPlus#exit
admin@XorPlus>exit
admin@XorPlus$
```

Step 3: Create a new bridge named br0.

```
admin@XorPlus$ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
```

Step 4: Add ports to br0.

```
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/1 -- set Interface te-1/1/1 type=pica8
admin@XorPlus$ovs-vsctl add-port br0 te-1/1/2 -- set Interface te-1/1/2 type=pica8
```

Step 5: enable L3-mode and the default table is 252

```
admin@XorPlus$ovs-vsctl set-l3-mode true
```

Step 6: Add a route flow

```
admin@XorPlus$ovs-ofctl add-flow br0 table=252,dl_vlan=1,dl_dst=22:00:00:00:00:00,ip,nw_dst=1.1.1.100/24,actions=se
```

Configuration Example2 in Crossflow Mode

In the following topology, we build a server network in a datacenter. The following requirements should be met:
● Servers should not be able to communicate with each other, which means traffic from a server can only be forwarded in the upstream direction.
●The network should be scalable, and the configuration of the switch should be simple (e.g., isolating the traffic between servers by ACLs or VLANs is too complex of a configuration). You can configure a ToR switch manually or by a controller—it's up to you.

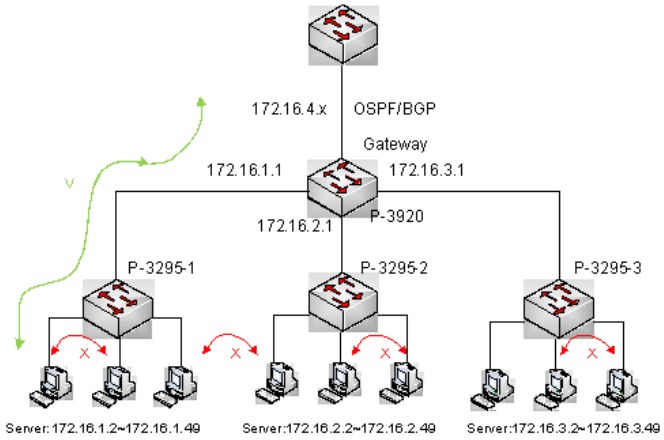


Figure 8-5. Crossflow network.

Configuring theP3295-1 switch

For P3295-1, configure ports ge-1/1/1~ge-1/1/48 in crossflow mode. Create 48 flows that will make traffic from the servers be forwarded only upstream, and be sure to configure flows that will forward the downstream traffic to the corresponding server.

```
admin@XorPlus# set interface stm firewall-table ingress  400
admin@XorPlus# set interface stm ipv4-route 6000
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow local-control false
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/49 crossflow local-control false
admin@XorPlus# commit
Waiting for merging configuration.
Commit OK.
Save done.
admin@XorPlus#
```

Create br0 and add ports to bridge.

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 ge-1/1/1
ovs-vsctl add-port br0 ge-1/1/2
ovs-vsctl add-port br0 ge-1/1/3
ovs-vsctl add-port br0 te-1/1/49
```

Add flows.

```
ovs-ofctl add-flow br0 in_port=1,actions=49
```

```
ovs-ofctl add-flow br0 in_port=49,nw_dst=172.16.1.2/32,actions=1
ovs-ofctl add-flow br0 in_port=2,actions=49
ovs-ofctl add-flow br0 in_port=49,nw_dst=172.16.1.3/32,actions=2
ovs-ofctl add-flow br0 in_port=3,actions=49
ovs-ofctl add-flow br0 in_port=49,nw_dst=172.16.1.4/32,actions=3
```

Configuring P3295-2 and P3295-3 switches

You can configure P3295-2 and P3295-3 using the instructions for configuring P3295-1.

Configuring the P3920 switch

For P3920, configure ports te-1/1/1~te-1/1/48 as a Layer 3 interfaces and enable the OSPF interface in xe-1/1/1. The interface xe-1/1/1 will join the OSPF network to the outside.

```
admin@XorPlus# set vlans vlan-id 100 l3-interface vlan100
admin@XorPlus# set vlans vlan-id 200 l3-interface vlan200
admin@XorPlus# set vlans vlan-id 300 l3-interface vlan300
admin@XorPlus# set vlans vlan-id 400 l3-interface vlan400
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 100
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 200
admin@XorPlus# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 300
admin@XorPlus# set interface gigabit-ethernet xe-1/1/1 family ethernet-switching native-vlan-id 400
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set l3-interface vlan-interface vlan100 address 172.16.1.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan200 address 172.16.2.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan300 address 172.16.3.1 prefix-length 24
admin@XorPlus# set l3-interface vlan-interface vlan400 address 172.16.4.1 prefix-length 24
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# set interface stm firewall-table ingress  400
admin@XorPlus# set interface stm ipv4-route 6000
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
XorPlus# set interface gigabit-ethernet te-1/1/1 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/2 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet te-1/1/3 crossflow enable true
admin@XorPlus# set interface gigabit-ethernet xe-1/1/1 crossflow enable true
admin@XorPlus# commit
Commit OK.
Save done.
```

Be sure to configure the OSPF interface to work with the OSPF Layer 3 network.

```
admin@Xorplus# set protocols ospf interface vlan400 area 0.0.0.0
admin@XorPlus# set protocols ospf router-id 1.1.1.1
admin@XorPlus# set protocols ospf redistribute connected
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

Create br0 and add ports to br0

```
ovs-vsctl add-br br0
ovs-vsctl add-port br0 te-1/1/1 - set interface te-1/1/1 type=crossflow
ovs-vsctl add-port br0 te-1/1/2 - set interface te-1/1/2 type=crossflow
ovs-vsctl add-port br0 te-1/1/3 - set interface te-1/1/1 type=crossflow
ovs-vsctl add-port br0 xe-1/1/1 - set interface xe-1/1/1 type=crossflow
```

Add flows.

```
ovs-ofctl add-flow br0 in_port=1,actions=set_field:22:22:22:22:22:22-\>dl_dst,49
ovs-ofctl add-flow br0 in_port=2,actions=set_field:22:22:22:22:22:22-\>dl_dst,49
```

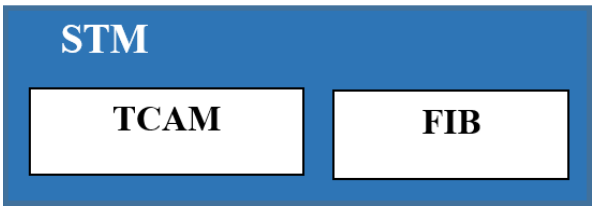
```
ovs-ofctl add-flow br0 in_port=3,actions=set_field:22:22:22:22:22:22-\>dl_dst,49
```

Example for Configuring STM Resource Allocation

Shared Table Memory (STM), is a feature designed to allow sharing a common resource across several table memories. This provides a large number of shared resources that can be allocated depending on the intended user application. It allows allocating resources to tables as needed instead of in fixed proportions, enabling large tables to receive more resources.

As shown in Figure 1, STM resource space includes two parts: TCAM and FIB. TCAM and FIB resources were separate entities of fixed size. If a given system application did not utilize one of these resources, then the entries remained unused and could not be reclaimed for other purpose. This document describes an example of how to configure TCAM and FIB resource allocation.

Figure 1. Shared Table Memory



TCAM

The TCAM resource is used to configure ACL entries and OpenFlow entries which contain the following parts:

- User defined firewall tables including ingress and egress tables, which occupy the TCAM resource.
- Resources reserved for the ACL entries for the Control Plane Policing (CoPP) and MAC Authentication Bypass (MAB).
- OpenFlow flow table resources.

You can use the CLI command to configure the maximum number of entries in the user-defined firewall tables that are allocated in TCAM. The remaining TCAM system resources are used for OpenFlow flow tables and the system reserved TCAM resource for ACL entries of COPP. In the result of this is that after the resources reserved by the system for the COPP and MAB are exhausted, it will go onto to allocate more memory resource from the free OpenFlow resources. But the space allocated through CLI for the user-defined firewall tables remains unaffected even if there is free space in it in case space runs out for CoPP and MAB or the OpenFlow tables.

NOTE :

CoPP firewall table occupies the egress firewall table resource.

In CrossFlow mode, by default, the system allocates all TCAM resources to the L2/L3 firewall tables except the resources reserved for COPP and the MAB. Take AS5812_54T switch (ASIC is Trident2+) as an example.

```
admin@Xorplus# set interface stm firewall-table egress
Possible completions:
  [0..512]                       Max Egress ACL Counter
admin@Xorplus# set interface stm firewall-table ingress
Possible completions:
  [0..768]                       Max Ingress ACL Counter
```

We can see that the total number of TCAM resource is 512+768=1280 entries (which do not include the resources reserved for CoPP and MAB), are all allocated to L2/L3 firewall tables by default. In this case, there is no resource left to configure OpenFlow flow tables. If you want to configure OpenFlow flow tables, you need to modify the number of resources allocated to the firewall tables. For example, we can commit the following configurations:

```
admin@Xorplus# set interface stm firewall-table ingress 100
admin@Xorplus# set interface stm firewall-table egress 300
admin@Xorplus# commit
```

The above configurations have allocated up to 100 ingress ACL entries and 300 egress ACL entries in TCAM. The remaining system resources in TCAM are 1280-100-300=880, which is the maximum resource that can be used for OpenFlow flow entries.

FIB Table Resources

The L2/L3 entry tables are allocated in the FIB of the dedicated memory space in STM. The MAC table occupies the FDB resource; the IPv4 route table and IPv6 route table occupy the routing table resource. The STM share mode, can be set by using **set interface stm share-mode** command. It determines the fixed resource size for these L2/L3 entry tables in the FIB.

Taking the Trident2+ switch as an example, we can see that under different share modes, the dedicated resource allocation of each L2/host-route/route entries in the STM is different.

```
admin@Xorplus# set interface stm share-mode
Possible completions:
  0                              l2-size 294912, host-route 12000, route 12000
  1                              l2-size 229376, host-route 44800, route 12000
  2                              l2-size 163840, host-route 70400, route 12000
  3                              l2-size 98304,  host-route 96000, route 12000
  4                              l2-size 32768,  host-route 12000, route 115200
```

```
  5                              l2-size 32768,  host-route 12000, route 12000
```

In CrossFlow mode, user can enable L2/L3 mode as a PICOS OVS multi-table function. If the L2/L3 mode is enabled, the FIB table resource will be shared by legacy ports and CrossFlow ports (see description in Crossflow Mode Introduction), in a way that will prevent mixing of data traffic between the different types of ports.

User can allocate the FIB resource for special ports as the following command shows.

```
admin@Xorplus# set interface stm share-mode 3
admin@Xorplus# set interface stm mac-table 20000
admin@Xorplus# set interface stm ipv4-route 6000
admin@Xorplus# set interface stm ipv6-route 1000
admin@Xorplus# commit
```

The second command, **set interface stm mac-table 20000**, allocates the FDB table resource for legacy ports, and the rest of the resource for CrossFlow ports and OpenFlow ports.

The last two commands, **set interface stm ipv4-route 6000**, and **set interface stm ipv6-route 1000**, allocates the route table resource for legacy ports, and the rest of resources for CrossFlow ports and OpenFlow ports.

After the configurations are committed, we can use the **run show interface stm** command line to view the STM resource allocation:

```
admin@Xorplus# run show interface stm
Total stm resource:
  Share-mode: 3
  number of host routes: 96000
  number of mac unicast addresses: 20000
  number of firewall ingress tables: 100
  number of firewall egress tables: 300
  number of IPv4 unicast routes: 6000
  number of IPv6 unicast routes: 1000
Stm resource in use:
  number of firewall ingress tables: 0
  number of firewall egress tables: 21
```

The item **number of firewall egress tables** is used for describing STM resources for CoPP. By default, the value of number of firewall egress tables in STM resource in use: is 21 as have been used by the default CoPP configurations.

Multi-action in crossflow mode

From version 4.1.1,pica8 switch support multi-action in crossflow mode. Before supporting this ,there is a issue. When the host forward the packet to others, first packet is forwarded to SDN Controller. This is caused “ONE” packet loss every time when the host forward the packet, and without OF rule, the SDN Controller can not update the device information (IP/MAC).That is why we want to support when the packet is forwarded to PicOS, the action should be supported both “go to Controller” and “Normal” at the same time

Command

ovs-ofctl add-flow br0 in_port=5,actions=normal,controller

Example

prerequisites

xorplus configurations:

```
admin@Xorplus# show|display set

set interface gigabit-ethernet ge-1/1/5 crossflow enable true

set interface gigabit-ethernet ge-1/1/5 family ethernet-switching port-mode "trunk"

set interface gigabit-ethernet ge-1/1/5 family ethernet-switching vlan members 200

set interface gigabit-ethernet ge-1/1/6 crossflow enable true

set interface gigabit-ethernet ge-1/1/6 family ethernet-switching port-mode "trunk"

set interface gigabit-ethernet ge-1/1/6 family ethernet-switching vlan members 200

set interface gigabit-ethernet ge-1/1/7 crossflow enable true

set interface gigabit-ethernet ge-1/1/7 family ethernet-switching port-mode "trunk"

set interface gigabit-ethernet ge-1/1/7 family ethernet-switching vlan members 200

set protocols spanning-tree enable false

set system log-level "trace"

set vlans vlan-id 200

set xovs enable true

set xovs special-packets-options sequence 123 match destination-mac-address 22:22:22:22:22:22

set xovs special-packets-options sequence 123 match ether-type 2048

set xovs special-packets-options sequence 123 handler "both"
```

ovs configurations:

```
ovs-vsctl set-controller br0 tcp:10.10.51.42:6633

ovs-vsctl add-port br0 ge-1/1/5 -- set interface ge-1/1/5 type=crossflow

ovs-vsctl add-port br0 ge-1/1/6 -- set interface ge-1/1/6 type=crossflow

ovs-vsctl add-port br0 ge-1/1/7 -- set interface ge-1/1/7 type=crossflow
```

start controller

ryu-manager ….py

add flow with normal and controller

step1,configurations are the same with prerequisites

step2,add flow

ovs-ofctl add-flow br0 in_port=5,actions=normal,controller

step3:send packets

send ip packets with dst mac 22:22:22:22:22:22,type is 0x0800,vlan is 200,src ip 1.1.1.200,dst ip is 5.5.5.200 to ge-1/1/5.

Result:ge-1/1/6 and ge-1/1/7 will transmit packets.And the packets are sending to cpu(500pps). Packet-in packets' data is the same with the original packets from ge-1/1/5

PICOS Routing and Switching Command Reference

Command-Line Interface Commands

- copy running-config startup-config
- set cli idle-timeout
- set cli screen-length
- set cli terminal
- syslog monitor
- syslog notify
- hwclock
- rollback

System Management Commands

- NAC Configuration Commands
  - set protocols dot1x aaa radius authentication server-ip
  - set protocols dot1x aaa radius authentication server-ip priority
  - set protocols dot1x aaa radius authentication server-ip retry-num
  - set protocols dot1x aaa radius authentication server-ip retry-interval
  - set protocols dot1x aaa radius authentication server-ip detect-interval
  - set protocols dot1x interface auth-mode 802.1x
  - set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
  - set protocols dot1x interface auth-mode mac-radius
  - set protocols dot1x interface auth-mode web
  - set protocols dot1x interface authentication-open disable
  - set protocols dot1x aaa radius dynamic-author client
  - set protocols dot1x aaa radius dynamic-author client shared-key
  - set protocols dot1x aaa radius nas-ip
  - set protocols dot1x aaa radius accounting disable
  - set protocols dot1x interface host-mode
  - set protocols dot1x block-vlan-id
  - set protocols dot1x server-fail-vlan-id
  - set protocols dot1x filter sequence from destination-address-ipv4
  - set protocols dot1x filter sequence from destination-address-ipv6
  - set protocols dot1x filter sequence from destination-port
  - set protocols dot1x filter sequence from ether-type
  - set protocols dot1x filter sequence from source-address-ipv4
  - set protocols dot1x filter sequence from source-address-ipv6
  - set protocols dot1x filter sequence from source-port
  - set protocols dot1x filter sequence from protocol
  - set protocols dot1x filter sequence then action
  - run show dot1x all
  - run show dot1x interface
  - run show dot1x server
  - run show dot1x dynamic filter
  - run show dot1x downloadable filter
  - run show dot1x interface statistics gigabit-ethernet
  - set protocols dot1x server-fail recovery-method
  - set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
  - set protocols dot1x aaa vrf mgmt-vrf
  - set protocols dot1x interface session-timeout
  - set protocols dot1x interface recovery-timeout
  - set protocols dot1x server-fail recovery-timeout
  - set protocols dot1x interface max-sessions
  - set protocols dot1x max-sessions-per-port
  - set protocols dot1x aaa radius authentication server-ip auth-port
  - set protocols dot1x aaa radius authentication server-ip acct-port
  - set protocols dot1x aaa radius dynamic-author client port
  - run show dot1x radius-port
  - set protocols dot1x filter sequence from destination-mac-address
  - set protocols dot1x filter sequence from vlan
- SNMP Configuration Commands
  - set protocols snmp trap-group targets security-name
  - set protocols lldp snmp-trap
  - set protocols snmp trap-group event cpu-threshold enable
  - set protocols snmp trap-group event cpu-threshold high

    - set protocols snmp trap-group event cpu-threshold interval
    - set protocols snmp trap-group event cpu-threshold low
    - set protocols snmp trap-group event mac-threshold enable
    - set protocols snmp trap-group event mac-threshold interval
    - set protocols snmp trap-group event mac-threshold limit
    - set protocols snmp trap-group vrf mgmt-vrf
    - set protocols snmp trap-group version
    - set protocols snmp v3 enable
    - set protocols snmp v3 usm-user
    - set protocols snmp v3 usm-user group
    - set protocols snmp v3 group notify-view
    - set protocols snmp v3 group read-view
    - set protocols snmp v3 group write-view
    - set protocols snmp v3 group security-level
    - set protocols snmp v3 usm-user authentication-mode
    - set protocols snmp v3 usm-user authentication-key
    - set protocols snmp v3 usm-user privacy-mode
    - set protocols snmp v3 usm-user privacy-key
    - set protocols snmp v3 mib-view subtree mask
    - set protocols snmp v3 mib-view subtree type
    - set protocols snmp trap-group source-interface
    - set protocols snmp community
    - set protocols snmp community authorization
    - set protocols snmp community clients
    - set protocols snmp contact
    - set protocols snmp location
    - run show snmp statistics
- Mirror Configuration Commands
    - set interface ethernet-switching-options analyzer input
    - set interface ethernet-switching-options analyzer output
    - set interface ethernet-switching-options analyzer erspan input
    - set interface ethernet-switching-options analyzer erspan output source-ip
    - set interface ethernet-switching-options analyzer erspan output dest-ip
    - set interface ethernet-switching-options analyzer erspan output vrf
    - run show analyzer
    - set firewall filter sequence then erspan source-ip
    - set firewall filter sequence then erspan dest-ip
    - set firewall filter sequence then erspan vrf
    - set firewall filter sequence then erspan ttl
- RMON Commands
    - run show rmon alarms
    - run show rmon eventlog
    - run show rmon events
    - run show rmon history
    - run show rmon statistics
    - set protocols snmp rmon alarm falling-event-index
    - set protocols snmp rmon alarm falling-threshold
    - set protocols snmp rmon alarm interval
    - set protocols snmp rmon alarm owner
    - set protocols snmp rmon alarm rising-event-index
    - set protocols snmp rmon alarm rising-threshold
    - set protocols snmp rmon alarm sample-type
    - set protocols snmp rmon alarm variable
    - set protocols snmp rmon event community
    - set protocols snmp rmon event description
    - set protocols snmp rmon event owner
    - set protocols snmp rmon event type
    - set protocols snmp rmon history buckets
    - set protocols snmp rmon history interface
    - set protocols snmp rmon history interval
    - set protocols snmp rmon history owner
    - set protocols snmp rmon statistics interface
    - set protocols snmp rmon statistics owner
- RESTCONF Commands
    - set protocols restconf
    - set protocols restconf port
    - set protocols restconf traceoptions flag config disable
    - set protocols restconf traceoptions flag all disable
    - set protocols restconf traceoptions flag datastore disable
- run show system boot-messages
- run show system connections

- run show system core-dumps
- run show system cpu-usage
- run show system date
- run show system fan
- run show system memory-usage
- run show system name
- run show system ntp-status
- run show system os
- run show system processes brief
- run show system processes detail
- run show system rollback compare to
- run show system rollback file
- run show system rollback list
- run show system rpsu
- run show system serial-number
- run show system temperature
- run show system uptime
- run show system users
- set system aaa local disable
- set system aaa radius accounting disable
- set system aaa radius accounting server-ip
- set system aaa radius accounting server-ip port
- set system aaa radius accounting server-ip shared-key
- set system aaa radius accounting server-ip timeout
- set system aaa radius authorization disable
- set system aaa radius authorization server-ip
- set system aaa radius authorization server-ip port
- set system aaa radius authorization server-ip shared-key
- set system aaa radius authorization server-ip timeout
- set system aaa radius vrf mgmt-vrf
- set system aaa tacacs-plus accounting
- set system aaa tacacs-plus authorization
- set system aaa tacacs-plus auth-type
- set system aaa tacacs-plus disable
- set system aaa tacacs-plus key
- set system aaa tacacs-plus port-number
- set system aaa tacacs-plus timeout
- set system aaa tacacs-plus server-ip
- set system aaa tacacs-plus source-interface
- set system aaa local-auth-fallback disable
- set system aaa tacacs-plus vrf mgmt-vrf
- set system hostname
- set system inband vlan-interface
- set system inband loopback
- set system inband routed-interface
- set system inband enable
- system login-acl network
- system login announcement
- system login user
- system login user admin class
- set system login user authentication plain-text-password
- system login user class
- set system timezone
- set system ntp server-ip
- set system ntp source-interface
- set system ntp vrf mgmt-vrf
- set interface gigabit-ethernet ptp mode
- set system services ssh connection-limit
- set system services ssh disable
- set system services ssh protocol-version v2
- set system services ssh rate-limit
- set system services ssh root-login
- set system services ssh idle-timeout
- set system services ssh port
- set system snmp-acl security-name network
- set system syslog server-ip
- set system syslog local-file
- set system syslog vrf mgmt-vrf
- set system usb disable
- set system management-ethernet eth0 ip-address {IPv4 | IPv6}

- set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}
- show system management-ethernet
- run request system reboot
- run show system hwinfo
- ping
- traceroute
- tftp
- set protocols sflow collector vrf mgmt-vrf
- scp
- set system login banner
- upgrade2 image-file
- upgrade2 image-file backup-file
- upgrade2 image-file factory-default
- upgrade2 image-file use-prev-config
- set system dns-server-ip
- set system console idle-timeout
- set system login multiline-banner message
- set system login multiline-announcement message
- set system aaa radius source-interface
- set protocols grpc enable
- set protocols grpc port
- set system ztp enable
- telnet
- set system start-shell-sh password
- set system services telnet disable
- set system services web disable

Interface Configuration Commands

- Port Security Commands
  - set interface gigabit-ethernet port-security mac-address vlan
  - set interface gigabit-ethernet port-security mac-limit
  - set interface gigabit-ethernet port-security sticky
  - set interface gigabit-ethernet port-security violation
  - set interface gigabit-ethernet port-security block
  - set interface ethernet-switching-options port-error-discard timeout
  - run show port-security brief
  - run show port-security address
  - run show port-security interface
  - run clear port-security port-error
  - run clear port-security sticky interface
  - run clear port-security sticky address
  - run clear port-security dynamic interface
  - run clear port-security dynamic address
- L3 Interface
  - set l3-interface vlan-interface vrf
  - set l3-interface vlan-interface address prefix-length
  - set l3-interface loopback address
  - set l3-interface loopback disable
  - set l3-interface loopback vrf
  - set l3-interface vlan-interface rate-limit
  - set l3-interface vlan-interface mtu
  - set l3-interface vlan-interface dhcp
  - run show l3-interface vlan-interface
  - run show l3-interface
  - run show l3-interface loopback
  - run clear l3-interface statistics
  - set l3-interface routed-interface dhcp
  - set l3-interface routed-interface rate-limit
  - set l3-interface routed-interface mtu
  - set l3-interface routed-interface vrf
  - set l3-interface routed-interface address
  - set l3-interface routed-interface description
  - run show l3-interface routed-interface
  - set l3-interface vlan-interface pmtu-discovery
  - set l3-interface routed-interface pmtu-discovery
- Routed Interface
  - run show interface routed-interface brief
  - run show vlans routed-vlan
  - set interface aggregate-ethernet routed-interface enable
  - set interface aggregate-ethernet routed-interface name
  - set interface aggregate-ethernet routed-interface sub-interface vlan-id

    - set interface gigabit-ethernet routed-interface enable
    - set interface gigabit-ethernet routed-interface sub-interface
    - set vlans reserved-vlan
    - set interface gigabit-ethernet routed-interface name
- set interface gigabit-ethernet speed
- Uplink Failure Detection Commands
    - run show interface ufd
    - set interface ufd link-to-monitor
    - set interface ufd link-to-disable
- IPv6 Neighbor Discovery Protocol Command Reference
    - set l3-interface routed-interface ipv6-nd adv-interval-option
    - set l3-interface routed-interface ipv6-nd home-agent-config-flag
    - set l3-interface routed-interface ipv6-nd home-agent-lifetime
    - set l3-interface routed-interface ipv6-nd home-agent-preference
    - set l3-interface routed-interface ipv6-nd managed-config-flag
    - set l3-interface routed-interface ipv6-nd mtu
    - set l3-interface routed-interface ipv6-nd other-config-flag
    - set l3-interface routed-interface ipv6-nd prefix off-link
    - set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
    - set l3-interface routed-interface ipv6-nd prefix router-address
    - set l3-interface routed-interface ipv6-nd prefix valid-lifetime
    - set l3-interface routed-interface ipv6-nd ra-fast-retrans
    - set l3-interface routed-interface ipv6-nd ra-interval
    - set l3-interface routed-interface ipv6-nd ra-lifetime
    - set l3-interface routed-interface ipv6-nd reachable-time
    - set l3-interface routed-interface ipv6-nd router-preference
    - set l3-interface routed-interface ipv6-nd suppress-ra
    - set l3-interface vlan-interface ipv6-nd adv-interval-option
    - set l3-interface vlan-interface ipv6-nd home-agent-config-flag
    - set l3-interface vlan-interface ipv6-nd home-agent-lifetime
    - set l3-interface vlan-interface ipv6-nd home-agent-preference
    - set l3-interface vlan-interface ipv6-nd managed-config-flag
    - set l3-interface vlan-interface ipv6-nd mtu
    - set l3-interface vlan-interface ipv6-nd other-config-flag
    - set l3-interface vlan-interface ipv6-nd prefix off-link
    - set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
    - set l3-interface vlan-interface ipv6-nd prefix router-address
    - set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
    - set l3-interface vlan-interface ipv6-nd ra-fast-retrans
    - set l3-interface vlan-interface ipv6-nd ra-interval
    - set l3-interface vlan-interface ipv6-nd ra-lifetime
    - set l3-interface vlan-interface ipv6-nd reachable-time
    - set l3-interface vlan-interface ipv6-nd router-preference
    - set l3-interface vlan-interface ipv6-nd suppress-ra
- set management-ethernet-speed eth0
- set interface gigabit-ethernet up-mode
- show interface bpdu-tunneling
- show interface aggregate-ethernet <lag_name>
- show interface aggregate-ethernet <lag_name> dot1q-tunneling
- show interface brief
- show interface detail
- show interface diagnostics optics all
- show interface ecmp max-path
- show interface flexlink
- show interface gigabit-ethernet <interface>
- set interface gigabit-ethernet fec
- set interface gigabit-ethernet family ethernet-switching vlan members
- set interface gigabit-ethernet family ethernet-switching port-mode
- set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol
- set interface gigabit-ethernet ether-options 802.3ad
- set interface gigabit-ethernet duplex auto
- set interface gigabit-ethernet breakout-type
- set interface gigabit-ethernet auto-speeds
- set interface ecmp hash-mapping field vlan disable
- set interface ecmp hash-mapping field port-source disable
- set interface ecmp hash-mapping field port-destination disable
- set interface ecmp hash-mapping field ip-source disable
- set interface ecmp hash-mapping field ip-protocol disable
- set interface ecmp hash-mapping field ip-destination disable
- set interface ecmp hash-mapping field ingress-interface disable
- set interface bpdu-tunneling destination-mac

- set interface aggregate-ethernet family ethernet-switching vlan members
- set interface aggregate-ethernet family ethernet-switching port-mode
- set interface aggregate-ethernet disable
- set interface aggregate-ethernet description
- set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout
- set interface aggregate-ethernet aggregated-ether-options lacp fallback enable
- set interface aggregate-ethernet aggregated-ether-options lacp
- set interface aggregate-ethernet
- run show interface port-index-mapping
- run show interface diagnostics tdr
- interface max-route-limit
- interface max-acl-rule-limit <egress/ingress>
- interface gigabit-ethernet <port> wred queue <value> min_thresh
- interface gigabit-ethernet <port> wred queue <value> max_thresh
- interface gigabit-ethernet <port> wred queue <value> enable
- interface gigabit-ethernet <port> wred queue <value> ecn_thresh
- interface gigabit-ethernet <port> wred queue <value> drop_probability
- interface gigabit-ethernet <port> storm-control <mode> ratio <value>
- interface gigabit-ethernet <port> storm-control <mode> pps
- interface gigabit-ethernet <port> storm-control <mode> kbps
- interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>
- interface gigabit-ethernet <port> snmp-trap
- interface gigabit-ethernet <port> power-preemphasis-level
- interface gigabit-ethernet <port> mtu
- interface gigabit-ethernet <port> mac-learning <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>
- interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged
- interface gigabit-ethernet <port> family ethernet-switching native-vlan-id
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress
- interface gigabit-ethernet <port> disable
- interface gigabit-ethernet <port> ether-options flow-control
- interface gigabit-ethernet <port> description
- interface gigabit-ethernet <port> crossflow local-control
- interface gigabit-ethernet <port> crossflow enable
- interface gigabit-ethernet <port> backup-port mode
- interface gigabit-ethernet <port> backup-port interface
- interface gigabit-ethernet <port> backup-port delay
- interface ethernet-switching-options mac-table-aging-time
- interface ethernet-switching-options buffer queue-limit
- interface ecmp max-path
- interface cut-through-mode
- interface aggregate-ethernet <lag_name> storm-control <mode> pps
- interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan
- interface aggregate-ethernet <lag_name> snmp-trap
- interface aggregate-ethernet <lag_name> mtu
- interface aggregate-ethernet <lag_name> hash-mapping mode
- interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress
- interface aggregate-ethernet <lag_name> crossflow local-control
- interface aggregate-ethernet <lag_name> crossflow enable
- interface aggregate-ethernet <lag_name> backup-port mode
- interface aggregate-ethernet <lag_name> backup-port interface
- interface aggregate-ethernet <lag_name> backup-port delay
- interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port
- interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control
- interface aggregate-balancing hash-mapping field vlan disable
- interface aggregate-balancing hash-mapping field port-source disable
- interface aggregate-balancing hash-mapping field port-destination disable
- interface aggregate-balancing hash-mapping field ip-source disable
- interface aggregate-balancing hash-mapping field ip-protocol disable
- interface aggregate-balancing hash-mapping field ip-destination disable
- interface aggregate-balancing hash-mapping field ingress-interface disable
- interface aggregate-balancing hash-mapping field ethernet-type disable

- interface aggregate-balancing hash-mapping field ethernet-source-address disable
- interface aggregate-balancing hash-mapping field ethernet-destination-address disable
- set interface ecmp hash-mapping randomized-load-balancing
- set interface ecmp hash-mapping round-robin-load-balancing
- set interface ecmp hash-mapping resilient-load-balancing
- set interface ecmp hash-mapping dlb-normal
- set interface ecmp hash-mapping symmetric
- set interface ecmp hash-mapping dlb-optimal
- set interface ecmp hash-mapping dlb-assigned
- set interface gigabit-ethernet breakout
- set interface gigabit-ethernet cdr

VLAN Configuration Commands

- set vlans dot1q-tunneling egress from
- set vlans dot1q-tunneling egress then action
- set vlans dot1q-tunneling egress then service-vlan
- set vlans dot1q-tunneling ingress from double-tag service-vlan
- set vlans dot1q-tunneling ingress from one-tag customer-vlan-list
- set vlans dot1q-tunneling ingress from untag enabled
- set vlans dot1q-tunneling ingress then
- set vlans vlan-id
- set vlans vlan-id description
- set vlans vlan-id l3-interface
- set vlans vlan-id vlan-name
- set vlans vlan-id private-vlan mode
- set vlans vlan-id private-vlan association
- set mac-map mac-address vlan
- run show vlans
- run show vlans private-vlan
- run show vlans private-vlan type
- run show mac-map
- set tracemac disable
- tracemac

Voice VLAN Configuration Commands

- set interface gigabit-ethernet voice-vlan mode
- set interface gigabit-ethernet voice-vlan tagged mode
- set interface gigabit-ethernet voice-vlan vlan-id
- set vlans voice-vlan aging
- set vlans voice-vlan dscp
- set vlans voice-vlan local-priority
- set vlans voice-vlan mac-address mask
- set vlans voice-vlan mac-address description
- show vlans voice-vlan
- show vlans voice-vlan oui
- show vlans voice-vlan vlan-id <text>

Layer 3 Routing Commands

- run show neighbors
- run show route
- run show route forward-host
- run show route forward-route
- run show vrf
- set ip vrf
- set ip routing enable
- set system management-vrf enable
- BGP Commands
  - run show bgp
  - run show bgp neighbor
  - run show bgp route
  - run show bgp unicast neighbor graceful-restart
  - set protocols bgp aggregate-address
  - set protocols bgp always-compare-med
  - set protocols bgp bestpath as-path type multipath-relax
  - set protocols bgp bestpath bandwidth
  - set protocols bgp bestpath compare-routerid
  - set protocols bgp bestpath med missing-as-worst
  - set protocols bgp cluster-id
  - set protocols bgp graceful-shutdown
  - set protocols bgp listen

- set protocols bgp local-as
- set protocols bgp max-med
- set protocols bgp multipath maximum-paths
- set protocols bgp neighbor activate
- set protocols bgp neighbor addpath-tx-all-paths
- set protocols bgp neighbor addpath-tx-bestpath-per-as
- set protocols bgp neighbor advertisement-interval
- set protocols bgp neighbor allowas-in
- set protocols bgp neighbor as-override
- set protocols bgp neighbor capability extended-nexthop
- set protocols bgp neighbor default-originate
- set protocols bgp neighbor description
- set protocols bgp neighbor disable-connected-check
- set protocols bgp neighbor ebgp-multihop
- set protocols bgp neighbor filter-list
- set protocols bgp neighbor next-hop-self
- set protocols bgp neighbor password
- set protocols bgp neighbor peer-group
- set protocols bgp neighbor prefix-list
- set protocols bgp neighbor remote-as
- set protocols bgp neighbor remove-private-as
- set protocols bgp neighbor route-map
- set protocols bgp neighbor route-reflector-client
- set protocols bgp neighbor send-community
- set protocols bgp neighbor shutdown
- set protocols bgp neighbor soft-reconfiguration
- set protocols bgp neighbor timers connect
- set protocols bgp neighbor timers holdtime
- set protocols bgp neighbor timers keepalive
- set protocols bgp neighbor ttl-security hops
- set protocols bgp neighbor update-source
- set protocols bgp network
- set protocols bgp network-import-check
- set protocols bgp peer-group
- set protocols bgp redistribute
- set protocols bgp route-map delay-timer
- set protocols bgp router-id
- set protocols bgp table-map
- set protocols bgp timers
- set protocols bgp update-delay
- set protocols bgp ebgp-requires-policy
- set protocols bgp neighbor timers delayopen
- set protocols bgp neighbor maximum-prefix
- set protocols bgp neighbor maximum-prefix-out
- set protocols bgp neighbor port
- set protocols bgp neighbor sender-as-path-loop-detection
- set protocols bgp fast-external-failover
- set protocols bgp confederation identifier
- set protocols bgp confederation peers
- set protocols bgp dampening
- set protocols bgp default local-preference
- set protocols bgp as-notation
- set protocols bgp neighbor local-as

- OSPFv2 Commands
  - run clear ospf interface
  - run show ospf border-routers
  - run show ospf database
  - run show ospf interface
  - run show ospf neighbor
  - run show ospf route
  - run show ospf summary-address
  - set protocols ospf aggregation timer
  - set protocols ospf area area-type
  - set protocols ospf area filter-list prefix
  - set protocols ospf area no-summary
  - set protocols ospf area range
  - set protocols ospf area virtual-link
  - set protocols ospf area virtual-link authentication
  - set protocols ospf area virtual-link authentication-key
  - set protocols ospf area virtual-link dead-interval
  - set protocols ospf area virtual-link hello-interval

- set protocols ospf area virtual-link message-digest-key md5
- set protocols ospf area virtual-link retransmit-interval
- set protocols ospf area virtual-link transmit-delay
- set protocols ospf auto-cost reference-bandwidth
- set protocols ospf compatible rfc1583
- set protocols ospf default-information originate
- set protocols ospf default-metric
- set protocols ospf interface area
- set protocols ospf interface authentication address
- set protocols ospf interface authentication message-digest
- set protocols ospf interface cost
- set protocols ospf interface dead-interval
- set protocols ospf interface hello-interval
- set protocols ospf interface message-digest-key md5
- set protocols ospf interface network
- set protocols ospf interface priority
- set protocols ospf interface retransmit-interval
- set protocols ospf interface transmit-delay
- set protocols ospf log-adjacency-changes
- set protocols ospf max-metric router-lsa administrative
- set protocols ospf max-metric router-lsa on-shutdown
- set protocols ospf max-metric router-lsa on-startup
- set protocols ospf multi-instance disable
- set protocols ospf network area
- set protocols ospf passive-interface
- set protocols ospf redistribute
- set protocols ospf redistribute metric-type
- set protocols ospf redistribute route-map
- set protocols ospf router-id
- set protocols ospf summary-address
- set protocols ospf timers lsa min-arrival
- set protocols ospf timers throttle spf
- set protocols ospf traceoption ism
- set protocols ospf traceoption lsa
- set protocols ospf traceoption nsm
- set protocols ospf traceoption packet
- set protocols ospf traceoption zebra
- set protocols ospf graceful-restart enable
- set protocols ospf capability opaque
- set protocols ospf graceful-restart grace-period
- set protocols ospf graceful-restart helper enable
- set protocols ospf graceful-restart helper planned-only
- set protocols ospf graceful-restart helper strict-lsa-checking
- set protocols ospf graceful-restart helper supported-grace-time
- run graceful-restart prepare ospf
- run show ospf graceful-restart helper
- set protocols ospf interface authentication-key

- OSPFv3 Command Reference
  - set protocols ospf6 area
  - set protocols ospf6 area range
  - set protocols ospf6 area stub
  - set protocols ospf6 area stub no-summary
  - set protocols ospf6 auto-cost reference-bandwidth
  - set protocols ospf6 distance
  - set protocols ospf6 distance-ospf6
  - set protocols ospf6 interface area
  - set protocols ospf6 interface cost
  - set protocols ospf6 interface dead-interval
  - set protocols ospf6 interface hello-interval
  - set protocols ospf6 interface ifmtu
  - set protocols ospf6 interface mtu-ignore
  - set protocols ospf6 interface network
  - set protocols ospf6 interface passive
  - set protocols ospf6 interface priority
  - set protocols ospf6 interface retransmit-interval
  - set protocols ospf6 interface transmit-delay
  - set protocols ospf6 log-adjacency-changes
  - set protocols ospf6 redistribute
  - set protocols ospf6 router-id
  - set protocols ospf6 stub-router administrative
  - set protocols ospf6 timers lsa min-arrival

- set protocols ospf6 timers throttle spf
- set protocols ospf6 traceoption
- set protocols ospf6 traceoption border-routers
- set protocols ospf6 traceoption lsa
- set protocols ospf6 traceoption message
- set protocols ospf6 traceoption neighbor
- set protocols ospf6 traceoption route
- set protocols ospf6 traceoption spf
- set protocols ospf6 traceoption zebra
- set protocols ospf6 graceful-restart enable
- set protocols ospf6 capability opaque
- set protocols ospf6 graceful-restart grace-period
- set protocols ospf6 graceful-restart helper enable
- set protocols ospf6 graceful-restart helper planned-only
- set protocols ospf6 graceful-restart helper lsa-checking-disable
- set protocols ospf6 graceful-restart helper supported-grace-time
- run graceful-restart prepare ospf6
- run show ospf6 graceful-restart helper

- Static Route Configuration Commands
  - set protocols static interface-route interface
  - set protocols static mroute
  - set protocols static route

- Route Map Commands
  - run show routing route-map
  - set routing as-path-list
  - set routing large-community-list expanded
  - set routing large-community-list standard
  - set routing prefix-list
  - set routing prefix-list description
  - set routing community-list expanded
  - set routing community-list standard
  - set routing extcommunity-list expanded
  - set routing extcommunity-list standard
  - set routing route-map set-action large-community
  - set routing route-map call
  - set routing route-map description
  - set routing route-map match as-path
  - set routing route-map match community
  - set routing route-map match community-with-exact-match
  - set routing route-map match evpn default-route
  - set routing route-map match evpn route-type
  - set routing route-map match evpn vni
  - set routing route-map match extcommunity
  - set routing route-map matching-policy
  - set routing route-map match interface
  - set routing route-map match ipv4-addr address
  - set routing route-map match ipv4-addr next-hop
  - set routing route-map match ipv4-addr route-source
  - set routing route-map match ipv6-addr
  - set routing route-map match large-community
  - set routing route-map match local-preference
  - set routing route-map match metric
  - set routing route-map match origin
  - set routing route-map match peer
  - set routing route-map match source-protocol
  - set routing route-map match source-vrf
  - set routing route-map match tag
  - set routing route-map on-match
  - set routing route-map set-action aggregator
  - set routing route-map set-action as-path exclude
  - set routing route-map set-action as-path prepend
  - set routing route-map set-action atomic-aggregate
  - set routing route-map set-action comm-list-delete
  - set routing route-map set-action community
  - set routing route-map set-action community-additive
  - set routing route-map set-action extcommunity
  - set routing route-map set-action extcommunity bandwidth
  - set routing route-map set-action extcommunity bandwidth-non-transitive
  - set routing route-map set-action ip-next-hop
  - set routing route-map set-action ipv4-vpn-next-hop
  - set routing route-map set-action ipv6-next-hop

- set routing route-map set-action label-index
- set routing route-map set-action large-comm-list-delete
- set routing route-map set-action local-preference
- set routing route-map set-action metric
- set routing route-map set-action metric-type
- set routing route-map set-action origin
- set routing route-map set-action originator-id
- set routing route-map set-action src
- set routing route-map set-action tag
- set routing route-map set-action weight

- Route Leaking Commands
  - BGP Route Leaking Commands
    - set protocols bgp ipv4-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf-route-map
    - set protocols bgp vrf ipv4-unicast import vrf
    - set protocols bgp vrf ipv4-unicast import vrf-route-map
    - set protocols bgp vrf ipv6-unicast import vrf
  - Static Route Leaking Commands
    - set protocols static route nexthop-vrf next-hop
    - set protocols static vrf route nexthop-vrf next-hop
- BFD Configuration Commands
  - run show bfd
  - run show bfd counters
  - run show bfd peers
  - set protocols bfd multihop peer local-address
  - set protocols bfd multihop peer local-address detect-multiplier
  - set protocols bfd multihop peer local-address minimum-ttl
  - set protocols bfd multihop peer local-address passive-mode
  - set protocols bfd multihop peer local-address receive-interval
  - set protocols bfd multihop peer local-address shutdown
  - set protocols bfd multihop peer local-address transmit-interval
  - set protocols bfd peer detect-multiplier
  - set protocols bfd peer echo-mode
  - set protocols bfd peer echo receive-interval
  - set protocols bfd peer echo transmit-interval
  - set protocols bfd peer local-address
  - set protocols bfd peer minimum-ttl
  - set protocols bfd peer passive-mode
  - set protocols bfd peer receive-interval
  - set protocols bfd peer shutdown
  - set protocols bfd peer transmit-interval
  - set protocols bfd profile
  - set protocols bfd profile detect-multiplier
  - set protocols bfd profile echo-mode
  - set protocols bfd profile echo receive-interval
  - set protocols bfd profile echo transmit-interval
  - set protocols bfd profile minimum-ttl
  - set protocols bfd profile passive-mode
  - set protocols bfd profile receive-interval
  - set protocols bfd profile shutdown
  - set protocols bfd profile transmit-interval
  - set protocols bgp bfd
  - set protocols ospf6 interface bfd
  - set protocols ospf interface bfd
  - set protocols pim interface bfd
- Policy-Based Routing (PBR) Commands
  - set routing pbr map sequence match destination-ipv4
  - set routing pbr map sequence match source-ipv4
  - set routing pbr map sequence match destination-port
  - set routing pbr map sequence match source-port
  - set routing pbr map sequence match destination-ipv6
  - set routing pbr map sequence match source-ipv6
  - set routing pbr map sequence action nexthop
  - set routing pbr map sequence action dscp
  - set routing pbr map sequence action nexthop-group
  - set routing nexthop-group nexthop-vrf nexthop
  - set routing pbr map vlan-interface
  - run show pbr map
  - run clear pbr map
- IPv4 Source Guard (IPSG for IPv4) Commands
  - set ip-source-guard binding ip

    - set ip-source-guard enable
    - set ip-source-guard verify
    - set ip-source-guard traceoptions enable
    - run show ip-source-guard binding
- IPv6 Source Guard (IPSG for IPv6) Commands
    - set ipv6-source-guard binding ip
    - set ipv6-source-guard enable
    - set ipv6-source-guard verify
    - set ipv6-source-guard traceoptions enable
    - run show ipv6-source-guard binding
- ND Inspection Commands
    - set protocols neighbour inspection vlan disable
    - set protocols neighbour inspection validate source-mac
    - set protocols neighbour inspection trust-port
    - run show nd inspection dhcp6-snooping binding
- ND Snooping Commands
    - set protocols neighbour snooping vlan enable
    - set protocols neighbour snooping trust-port
    - set neighbour snooping max-user-number
    - set protocols neighbour snooping static-prefix vlan
    - run show neighbor snooping
    - run show neighbor snooping prefix
    - run show neighbor snooping binding
    - run clear neighbor snooping prefix
    - run clear neighbor snooping binding
- IS-IS commands
    - set protocols isis area-tag network-entity
    - set protocols isis area-tag is-type
    - set protocols isis area-tag interface
    - set protocols isis area-tag hostname-dynamic
    - set protocols isis area-tag area-password authentication-type
    - set protocols isis area-tag area-password authentication-key
    - set protocols isis area-tag area-password authenticate-snp
    - set protocols isis area-tag domain-password authentication-type
    - set protocols isis area-tag domain-password authentication-key
    - set protocols isis area-tag domain-password authenticate-snp
    - set protocols isis area-tag attached-bit receive-ignore
    - set protocols isis area-tag attached-bit send
    - set protocols isis area-tag log-adjacency-changes
    - set protocols isis area-tag metric-style
    - set protocols isis area-tag set-overload-bit
    - set protocols isis area-tag purge-originator
    - set protocols isis area-tag lsp-mtu
    - set protocols isis area-tag lsp-timers gen-interval
    - set protocols isis area-tag lsp-timers refresh-interval
    - set protocols isis area-tag lsp-timers max-lifetime
    - set protocols isis area-tag spf-interval
    - set protocols isis area-tag spf-delay-ietf init-delay
    - set protocols isis area-tag spf-delay-ietf short-delay
    - set protocols isis area-tag spf-delay-ietf long-delay
    - set protocols isis area-tag spf-delay-ietf holddown
    - set protocols isis area-tag spf-delay-ietf time-to-learn
    - set protocols isis area-tag default-information originate
    - set protocols isis area-tag default-information originate metric
    - set protocols isis area-tag default-information originate route-map
    - set protocols isis area-tag topology ipv6-unicast
    - set protocols isis area-tag interface circuit-type
    - set protocols isis area-tag interface csnp-interval
    - set protocols isis area-tag interface psnp-interval
    - set protocols isis area-tag interface hello-padding
    - set protocols isis area-tag interface hello-interval
    - set protocols isis area-tag interface hello-multiplier
    - set protocols isis area-tag interface metric
    - set protocols isis area-tag interface network point-to-point
    - set protocols isis area-tag interface passive
    - set protocols isis area-tag interface password authentication-type
    - set protocols isis area-tag interface password authentication-key
    - set protocols isis area-tag interface priority
    - set protocols isis area-tag interface three-way-handshake
    - set protocols isis area-tag interface bfd
    - set protocols isis area-tag interface topology ipv6-unicast

- set protocols isis area-tag redistribute
- set protocols isis traceoption events
- set protocols isis traceoption adj-packets
- set protocols isis traceoption route-events
- set protocols isis traceoption snp-packets
- run show isis summary
- run show isis interface
- run show isis database
- run show isis hostname
- run show isis neighbor
- run show isis route
- run show isis topology

ACL Configuration Commands

- set firewall filter description
- set firewall filter input interface
- set firewall time-range periodic start
- set firewall time-range periodic end
- run show timerange
- run show filter
- set firewall filter sequence then dscp
- set firewall filter sequence then action
- set firewall filter sequence from destination-port
- set firewall filter sequence from protocol ip
- set firewall filter sequence from protocol ospf
- set firewall filter sequence description
- set firewall filter output interface
- set firewall filter input vlan-interface
- set firewall filter sequence from protocol udp
- set firewall filter sequence from destination-address-ipv6
- set firewall filter sequence then forwarding-class
- set firewall filter sequence from protocol tcp flags
- set firewall filter sequence from protocol igmp
- set firewall filter output routed-interface
- set firewall filter sequence log interval
- set firewall filter sequence from source-port
- set firewall filter output vlan-interface
- set firewall filter sequence from destination-address-ipv4
- set firewall system-output disable
- set firewall filter sequence from ip trust-mode
- set firewall filter sequence from source-mac-address
- set firewall filter sequence from destination-mac-address
- set firewall filter sequence from protocol tcp
- set firewall filter sequence from ip value
- set firewall filter input routed-interface
- set firewall filter sequence from protocol icmp
- set firewall filter sequence from protocol others
- set firewall filter sequence from ether-type
- set firewall filter sequence from vlan
- set firewall filter sequence from source-address-ipv6
- set firewall filter sequence from source-address-ipv4

QoS Configuration Commands

- set class-of-service forwarding-class local-priority
- set class-of-service scheduler mode
- set class-of-service interface default-priority
- set class-of-service classifier forwarding-class code-point
- set class-of-service interface classifier
- set class-of-service classifier
- set class-of–service classifier forwarding-class
- set class-of-service classifier trust-mode
- set class-of-service scheduler guaranteed-rate
- set class-of-service scheduler-profile forwarding-class scheduler
- set class-of-service scheduler weight
- set class-of-service easy-ecn mode
- set class-of-service interface scheduler-profile
- set class-of-service scheduler max-rate
- run show class-of-service interface
- CoPP Commands
  - set class-of-service scheduler max-bandwidth-pps

    - set class-of-service scheduler min-bandwidth-pps
    - set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
    - set class-of-service scheduler weight (CoPP)
    - set firewall filter copp sequence from destination-address-ipv4
    - set firewall filter copp sequence from destination-address-ipv6
    - set firewall filter copp sequence from destination-mac-address
    - set firewall filter copp sequence from destination-port
    - set firewall filter copp sequence from ether-type
    - set firewall filter copp sequence from protocol
    - set firewall filter copp sequence from source-address-ipv4
    - set firewall filter copp sequence from source-address-ipv6
    - set firewall filter copp sequence from source-mac-address
    - set firewall filter copp sequence from source-port
    - set firewall filter copp sequence from vlan
    - set firewall filter copp sequence then forwarding-class
    - set firewall filter copp sequence then dscp
    - run show copp bandwidth
    - run show copp statistics
    - run show interface stm
    - run clear copp statistics
    - set class-of-service forwarding-class local-priority (CoPP)
    - run show filter copp
- Buffer Management Commands
    - set interface ethernet-switching-options buffer egress-queue shared-ratio
    - set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
    - run show interface egress-buffer
    - run show interface gigabit-ethernet egress-queues
- Interface-based Rate Limiting Commands
    - set interface gigabit-ethernet rate-limiting ingress kilobits
    - set interface gigabit-ethernet rate-limiting ingress ratio
    - set interface gigabit-ethernet rate-limiting ingress burst
    - set interface gigabit-ethernet rate-limiting egress kilobits
    - set interface gigabit-ethernet rate-limiting egress ratio
    - set interface gigabit-ethernet rate-limiting egress burst
- ACL-based Traffic Policer Commands
    - set firewall policer if-exceeding count-mode
    - set firewall policer if-exceeding rate-limit
    - set firewall policer if-exceeding burst-limit
    - set firewall filter sequence then policer
    - set firewall policer if-exceeding action discard
    - run show policer
- PFC Commands
    - set class-of-service pfc-profile code-point drop
    - set class-of-service interface pfc-profile
    - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed
    - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio
    - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold
    - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset
    - set interface ethernet-switching-options buffer service-pool threshold
    - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom
    - set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio
    - set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold
    - set class-of-service pfc-watchdog granularity
    - set class-of-service pfc-watchdog restore-action
    - set class-of-service pfc-watchdog code-point detect-interval
    - set class-of-service pfc-watchdog code-point restore-interval
    - set class-of-service interface pfc-watchdog code-point enable
    - set class-of-service pfc-watchdog threshold period
    - set class-of-service pfc-watchdog threshold count
    - set class-of-service interface pfc-watchdog restore-mode
    - run clear class-of-service interface pfc-watchdog auto
    - run clear class-of-service interface pfc-watchdog manual
    - run show pfc-watchdog stats
    - run show pfc-watchdog config
    - run show interface gigabit-ethernet ingress-buffer
    - run show interface gigabit-ethernet egress-buffer
    - set class-of-service interface pfc-uplink-group
    - set class-of-service pfc-uplink-group original-dscp to-code-point
    - set class-of-service pfc-uplink-group original-dscp dscp

Protocol Configuration Commands

- set protocols arp interface address mac-address
- set protocols arp interface proxy
- set protocols arp inspection vlan disable
- set protocols arp inspection access-list ip mac-address
- set protocols arp inspection vlan access-list
- set protocols arp inspection trust-port
- run show arp inspection dhcp-binding
- run show arp inspection interface
- run show arp inspection vlan
- run show arp inspection access-list
- run show arp inspection statistics vlan
- set protocols arp aging-time
- set protocols lacp interface priority
- set protocols lacp priority
- set protocols sflow agent-id
- set protocols sflow collector udp-port
- set protocols sflow disable
- set protocols dhcp snooping vlan
- set protocols dhcp snooping trust-port
- set protocols dhcp snooping vlan option82-policy
- set protocols dhcp snooping option82 circuit-id
- set protocols dhcp snooping option82 remote-id
- set protocols dhcp snooping option82 trust-all
- set protocols dhcp snooping binding file
- set protocols dhcp snooping binding write-delay
- run show dhcp snooping binding
- set protocols dhcp relay interface disable
- set protocols dhcp relay interface dhcp-server-address
- set protocols dhcp relay interface relay-agent-address
- set protocols dhcp relay interface option82-policy
- set protocols dhcp relay option82 circuit-id
- set protocols dhcp relay option82 remote-id
- set protocols dhcp relay option82 trust-all
- set protocols dhcp server pool network
- set protocols dhcp server pool range low
- set protocols dhcp server pool range high
- set protocols dhcp server pool domain-name
- set protocols dhcp server pool dns-server
- set protocols dhcp server pool default-router
- set protocols dhcp server pool lease-time
- set protocols dhcp server pool vrf
- set protocols dhcp server pool tftp-server
- set protocols dhcp server pool log-server
- set protocols dhcp server pool bootfile-name
- run show dhcp server binding address
- run show dhcp server binding interface
- set protocols dhcp server interface disable
- set protocols dhcp6 relay interface disable
- set protocols dhcp6 relay interface destination
- set protocols dhcp6 relay interface remote-id
- run show dhcp6 relay-stats
- set protocols lacp interface rate
- run show lldp neighbor
- set protocols dhcp6 snooping vlan
- set protocols dhcp6 snooping trust-port
- set protocols dhcp6 snooping binding file
- set protocols dhcp6 snooping binding write-delay
- set protocols dhcp6 snooping vlan option-policy
- set protocols dhcp6 snooping option37 remote-id
- set protocols dhcp6 snooping option18 interface-id
- set protocols dhcp6 snooping interface max-clients
- run show dhcp6 snooping binding
- set protocols dhcp6 guard policy device-role
- set protocols dhcp6 guard policy trust-port
- set protocols dhcp6 guard policy interface
- set protocols dhcp6 guard policy preference-min
- set protocols dhcp6 guard policy preference-max
- set protocols dhcp6 guard policy match server source-address
- set protocols dhcp6 guard policy match reply ia-prefix

- run show dhcp6 guard policy
- run show dhcp6 guard
- run show arp
- set protocols sflow interface polling-interval
- set protocols sflow header-len
- set protocols sflow interface header-len
- set protocols sflow interfac sampling-rate egress
- set protocols sflow interface disable
- set protocols sflow interface sampling-rate ingress
- set protocols sflow polling-interval
- set protocols sflow sampling-rate egress
- set protocols sflow sampling-rate ingress
- set protocols sflow source-address

IP Multicast Commands

- IGMP Snooping Configuration Commands
  - run show igmp-snooping
  - run show igmp-snooping groups
  - run show igmp-snooping mrouter
  - run show igmp-snooping querier
  - set protocols igmp-snooping enable
  - set protocols igmp-snooping interface max-groups
  - set protocols igmp-snooping last-member-query-count
  - set protocols igmp-snooping last-member-query-interval
  - set protocols igmp-snooping max-response-time
  - set protocols igmp-snooping query-interval
  - set protocols igmp-snooping report-suppression
  - set protocols igmp-snooping robustness-variable
  - set protocols igmp-snooping vlan-id enable
  - set protocols igmp-snooping vlan-id fast-leave
  - set protocols igmp-snooping vlan-id mrouter interface
  - set protocols igmp-snooping vlan-id querier address
  - set protocols igmp-snooping vlan-id querier enable
  - set protocols igmp-snooping vlan-id querier other-querier-timer
  - set protocols igmp-snooping vlan-id querier version
  - set protocols igmp-snooping vlan-id static group interface
  - set protocols igmp-snooping vlan-id unregistered flood-all
- IGMP Commands
  - set protocols igmp interface
  - set protocols igmp interface join-group
  - set protocols igmp interface query-interval
  - set protocols igmp interface query-max-response-time
  - set protocols igmp interface version
  - run show igmp groups
  - run show igmp interface
- PIM Configuration Commands
  - set protocols pim ecmp
  - set protocols pim interface active-active
  - set protocols pim interface drpriority
  - set protocols pim interface hello holdtime
  - set protocols pim interface hello interval
  - set protocols pim interface sm
  - set protocols pim interface use-source
  - set protocols pim join-prune-interval
  - set protocols pim keep-alive-timer
  - set protocols pim packets
  - set protocols pim register-suppress-time
  - set protocols pim rp
  - set protocols pim spt-switchover infinity-and-beyond
  - set protocols pim ssm prefix-list
  - set protocols pim interface bsm
  - set protocols pim interface unicast-bsm
  - run show pim interface
  - run show pim rp-info
  - run show pim neighbor
  - run show pim upstream
  - run show mroute
  - mtrace
  - run show pim group-type
  - run show pim bsr
  - run show pim bsm-database

- run show pim bsrp-info
- run clear pim bsr-data

- Multicast Source Discovery Protocol (MSDP) Commands
  - set protocols msdp mesh-group source
  - set protocols msdp mesh-group member
  - run show msdp mesh-group
  - run show msdp peer
  - run show msdp sa
- Multicast VLAN Registration (MVR) Commands
  - run show igmp-snooping mvr mvlan
  - run show igmp-snooping mvr receiver-vlan
  - set protocols igmp-snooping vlan-id mvr receiver vlan-list
  - set protocols igmp-snooping vlan-id mvr source group

OpenFlow Commands in CrossFlow Mode

VXLAN Commands

- set vxlans source-interface address
- OVSDB VTEP command
  - set protocols ovsdb controller vrf mgmt-vrf
  - set protocols ovsdb controller address
  - set protocols ovsdb controller inactivity-probe-duration
  - set protocols ovsdb controller maximum-backoff-duration
  - set protocols ovsdb controller port
  - set protocols ovsdb controller protocol
  - set protocols ovsdb interface
  - set protocols ovsdb management-ip
  - set protocols ovsdb ssl bootstrap
  - set protocols ovsdb ssl ca-cert
  - set protocols ovsdb ssl certificate
  - set protocols ovsdb ssl private-key
- set vxlans l3-vni prefix-routes-only
- set vxlans vni mcast-group
- run show vxlan statistics
- run clear vxlan statistics
- set vxlans udp-port
- run show vxlan vni
- run show vxlan address-table
- run show vxlan arp
- run show vxlan l3-vni entry
- run show vxlan neighbor
- set vxlans vni decapsulation mode
- set vxlans vni encapsulation mode
- set vxlans vni encapsulation vlan
- set vxlans vni flood vtep
- set vxlans vni flood vtep mac-address
- set vxlans vni flood vtep traffic-type
- set vxlans vni vlan
- set vxlans tunnel-mac-leaning disable
- set vxlans l3-vni

BGP EVPN Commands

- run show bgp evpn summary
- run show bgp evpn import-rt
- run show bgp evpn vrf-import-rt
- run show bgp evpn vni
- run show evpn es
- run show evpn access-vlan
- run show evpn arp-cache
- run show evpn next-hops
- run show evpn rmac
- run show evpn mac vni
- set interface aggregate-ethernet evpn mh es-df-pref
- set interface aggregate-ethernet evpn mh es-id
- set interface aggregate-ethernet evpn mh es-sys-mac
- set l3-interface routed-interface router-mac
- set l3-interface vlan-interface anycast address
- set l3-interface vlan-interface anycast mac
- set l3-interface vlan-interface router-mac
- set protocols bgp evpn advertise-default-gw
- set protocols bgp evpn advertise ipv4-unicast

- set protocols bgp evpn advertise ipv6-unicast
- set protocols bgp evpn advertise-svi-ip
- set protocols bgp evpn default-originate
- set protocols bgp evpn disable-ead-evi-rx
- set protocols bgp evpn disable-ead-evi-tx
- set protocols bgp evpn vni
- set protocols bgp evpn vni advertise-default-gw
- set protocols bgp evpn vni advertise-svi-ip
- set protocols bgp evpn vni rd
- set protocols bgp evpn vni route-target type
- set protocols bgp neighbor evpn activate
- set protocols bgp neighbor evpn allowas-in
- set protocols bgp neighbor evpn route-map
- set protocols bgp neighbor evpn route-reflector-client
- set protocols bgp vrf evpn advertise-pip ip
- set protocols evpn mh mac-holdtime
- set protocols evpn mh redirect-off
- set protocols evpn mh startup-delay
- set vxlans vni arp-nd-suppress disable
- set protocols bgp evpn advertise-all-vni
- set protocols evpn mh neigh-holdtime
- run show bgp evpn route
- run show bgp evpn route detail
- run show bgp evpn route vni
- run show bgp evpn route rd
- run show bgp evpn route type

PoE Configuration Commands

- set poe interface max-power
- set poe interface detection-type
- set poe interface enable
- set poe interface mode
- set poe interface priority
- set poe interface threshold-mode
- set poe power management-mode
- set poe power mode
- set poe interface lldp-negotiation
- set poe power voltage
- set poe traceoptions flag all disable
- run show poe interface
- run show poe power
- set poe perpetual-power enable

VRRP Commands

- set protocols vrrp interface vrid
- set protocols vrrp interface vrid disable
- set protocols vrrp interface vrid version
- set protocols vrrp interface vrid ip
- set protocols vrrp interface vrid priority
- set protocols vrrp interface vrid interval
- set protocols vrrp interface vrid preempt enable
- set protocols vrrp interface vrid load-balance disable
- set protocols vrrp interface vrid load-balance virtual-mac time-interval
- set protocols vrrp interface vrid accept disable
- set protocols vrrp interface vrid authentication type
- set protocols vrrp interface vrid simple-key
- set protocols vrrp interface vrid md5-key
- run show vrrp
- set protocols vrrp interface vrid ipv6-nd adv-interval-option
- set protocols vrrp interface vrid ipv6-nd home-agent-config-flag
- set protocols vrrp interface vrid ipv6-nd home-agent-lifetime
- set protocols vrrp interface vrid ipv6-nd home-agent-preference
- set protocols vrrp interface vrid ipv6-nd managed-config-flag
- set protocols vrrp interface vrid ipv6-nd mtu
- set protocols vrrp interface vrid ipv6-nd other-config-flag
- set protocols vrrp interface vrid ipv6-nd prefix off-link
- set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix router-address
- set protocols vrrp interface vrid ipv6-nd ra-fast-retrans

- set protocols vrrp interface vrid ipv6-nd ra-interval
- set protocols vrrp interface vrid ipv6-nd ra-lifetime
- set protocols vrrp interface vrid ipv6-nd reachable-time
- set protocols vrrp interface vrid ipv6-nd router-preference
- set protocols vrrp interface vrid ipv6-nd suppress-ra

Spanning Tree Protocol Commands

- run show spanning-tree
- run show spanning-tree mstp
- run show spanning-tree pvst
- run show spanning-tree rstp
- run show spanning-tree statistics
- run show spanning-tree stp
- set protocols spanning-tree enable
- set protocols spanning-tree force-version
- set protocols spanning-tree interface enable
- set protocols spanning-tree mstp bridge-priority
- set protocols spanning-tree mstp configuration-name
- set protocols spanning-tree mstp forward-delay
- set protocols spanning-tree mstp hello-time
- set protocols spanning-tree mstp interface bpdu-filter
- set protocols spanning-tree mstp interface bpdu-guard
- set protocols spanning-tree mstp interface edge
- set protocols spanning-tree mstp interface external-path-cost
- set protocols spanning-tree mstp interface internal-path-cost
- set protocols spanning-tree mstp interface manual-forwarding
- set protocols spanning-tree mstp interface mode
- set protocols spanning-tree mstp interface port-priority
- set protocols spanning-tree mstp interface root-guard
- set protocols spanning-tree mstp interface tcn-guard
- set protocols spanning-tree mstp max-age
- set protocols spanning-tree mstp max-hops
- set protocols spanning-tree mstp msti bridge-priority
- set protocols spanning-tree mstp msti interface cost
- set protocols spanning-tree mstp msti interface port-priority
- set protocols spanning-tree mstp revision-level
- set protocols spanning-tree mstp msti vlan
- set protocols spanning-tree pvst interface bpdu-guard
- set protocols spanning-tree pvst interface manual-forwarding
- set protocols spanning-tree pvst interface mode
- set protocols spanning-tree pvst interface root-guard
- set protocols spanning-tree pvst vlan bridge-priority
- set protocols spanning-tree pvst vlan enable
- set protocols spanning-tree pvst vlan forward-delay
- set protocols spanning-tree pvst vlan hello-time
- set protocols spanning-tree pvst vlan interface path-cost
- set protocols spanning-tree pvst vlan interface port-priority
- set protocols spanning-tree pvst vlan max-age
- set protocols spanning-tree rstp bridge-priority
- set protocols spanning-tree rstp forward-delay
- set protocols spanning-tree rstp hello-time
- set protocols spanning-tree rstp interface bpdu-filter
- set protocols spanning-tree rstp interface bpdu-guard
- set protocols spanning-tree rstp interface edge
- set protocols spanning-tree rstp interface mode
- set protocols spanning-tree rstp interface path-cost
- set protocols spanning-tree rstp interface port-priority
- set protocols spanning-tree rstp interface root-guard
- set protocols spanning-tree rstp interface tcn-guard
- set protocols spanning-tree rstp max-age
- set protocols spanning-tree stp bridge-priority
- set protocols spanning-tree stp forward-delay
- set protocols spanning-tree stp hello-time
- set protocols spanning-tree stp interface bpdu-filter
- set protocols spanning-tree stp interface bpdu-guard
- set protocols spanning-tree stp interface edge
- set protocols spanning-tree stp interface mode
- set protocols spanning-tree stp interface path-cost
- set protocols spanning-tree stp interface port-priority
- set protocols spanning-tree stp interface root-guard

- set protocols spanning-tree stp interface tcn-guard
- set protocols spanning-tree stp max-age

MLAG Commands

- set protocols mlag domain
- set protocols mlag domain node
- set protocols mlag domain interface link
- set protocols mlag domain peer-ip peer-link
- set protocols mlag domain peer-ip peer-vlan
- run show mlag domain
- run show mlag link
- run show mlag consistency-parameter

GRE Tunnel Interface Commands

- run show l3-interface tunnel
- set l3-interface tunnel address
- set l3-interface tunnel destination
- set l3-interface tunnel disable
- set l3-interface tunnel source
- set l3-interface tunnel tunnel-mode gre-ip
- set l3-interface tunnel vrf

GVRP Commands

- set protocols gvrp join-timer
- set protocols gvrp leave-timer
- set protocols gvrp leaveall-timer
- run clear gvrp interface statistics
- run show gvrp interface
- run show gvrp interface statistics
- set protocols gvrp edge-switch
- set protocols gvrp enable
- set protocols gvrp interface enable
- set protocols gvrp traceoptions flag config
- set protocols gvrp traceoptions flag packets

MVRP Commands

- run clear mvrp interface statistics
- run show mvrp interface
- run show mvrp interface statistics
- set protocols mvrp edge-switch
- set protocols mvrp enable
- set protocols mvrp interface enable
- set protocols mvrp traceoptions flag config
- set protocols mvrp traceoptions flag packets
- set protocols mvrp join-timer
- set protocols mvrp leave-timer
- set protocols mvrp leaveall-timer

ERPS Commands

- run show erps brief
- run show erps interface
- run show erps ring
- run show erps statistics
- set protocols erps ring
- set protocols erps version
- set protocols erps enable
- set protocols erps ring instance
- set protocols erps ring instance control-vlan
- set protocols erps ring instance description
- set protocols erps ring instance enable
- set protocols erps ring instance guard-timer
- set protocols erps ring instance holdoff-timer
- set protocols erps ring instance protected-instance
- set protocols erps ring instance r-aps level
- set protocols erps ring instance rpl
- set protocols erps ring instance wtr-timer
- set protocols erps ring port0 interface
- set protocols erps ring port1 interface
- set protocols erps ring r-aps ring-mac

- set protocols erps ring sub-ring
- set protocols erps ring virtual-channel
- set protocols erps ring instance non-revertive
- set protocols erps tcn-propagation
- set protocols erps ring instance connect ring
- erps switch force ring instance
- erps switch manual ring instance
- erps clear ring ring instance
- set protocols erps traceoptions flag all disable
- set protocols erps traceoptions flag config disable
- set protocols erps traceoptions flag ring disable

EFM OAM Commands

- set protocols ethernet-oam interface enable
- set protocols ethernet-oam interface mode
- set protocols ethernet-oam interface remote-loopback supported
- set protocols ethernet-oam interface remote-loopback timeout
- ethernet-oam remote-loopback start|stop interface
- set protocols ethernet-oam interface timeout
- set protocols ethernet-oam traceoptions flag packets
- set protocols ethernet-oam traceoptions flag config
- run show ethernet-oam
- run show ethernet-oam statistics

MPLS Commands

- set protocols mpls interface
- set protocols mpls ldp router-id
- set protocols mpls ldp ordered-control
- set protocols mpls ldp neighbor password
- set protocols mpls ldp neighbor session-holdtime
- set protocols mpls ldp neighbor ttl-security disable
- set protocols mpls ldp neighbor ttl-security hops
- set protocols mpls ldp interface
- set protocols mpls ldp ttl-security disable (IP family)
- set protocols mpls ldp label-local-advertise
- set protocols mpls ldp label-local-allocate
- set protocols mpls ldp discovery transport-address
- set protocols mpls ldp discovery hello-interval
- set protocols mpls ldp discovery hello-holdtime
- set protocols mpls ldp discovery targeted-hello-interval
- set protocols mpls ldp discovery targeted-hello-holdtime
- set protocols mpls ldp discovery targeted-hello-accept
- set protocols mpls ldp dual-stack transport-connection prefer-ipv4
- set protocols mpls ldp dual-stack interop
- set protocols mpls ldp targeted-neighbor
- set protocols mpls ldp traceoption labels
- set protocols mpls ldp traceoption errors
- set protocols mpls ldp traceoption event
- set protocols mpls ldp traceoption discovery
- set protocols mpls ldp traceoption messages
- run show mpls ldp binding
- run show mpls ldp neighbor
- run show mpls ldp interface
- run show mpls forward-table
- run show mpls egress interface
- run show mpls table
- run show mpls interface
- run show mpls status
- run show mpls label
- run show mpls ldp discovery
- run show mpls fec

Loopback Detection Commands

- set protocols loopback-detection enable
- set protocols loopback-detection interface enable
- set protocols loopback-detection message-interval
- set protocols loopback-detection traceoptions configuration disable
- set protocols loopback-detection traceoptions all disable
- run show loopback-detection

- run clear loopback-detection interface

Command-Line Interface Commands

The section provides the commands about command-line interface operation.

- copy running-config startup-config
- set cli idle-timeout
- set cli screen-length
- set cli terminal
- syslog monitor
- syslog notify
- hwclock
- rollback

copy running-config startup-config

The **copy running-config startup-config** command saves the running configuration file from the RAM to the flash.

> **Warning:**
>
> This command is supported only on FS S5810 Series, S3410 Series and S5860 Series switches, and you have to do configuration saving by running this command. This specific save command is requested by hardware vendor due to the Flash limitation on numbers of write/erase cycles.

Command Syntax

copy running-config startup-config

Parameter

None.

Usage Guidelines

When performing the following operations, you need to manually issue the configuration saving command to save the configuration file from the RAM to the flash.

- Perform picos_boot
- Set L2 / L3 CLI commands (for the L2 / L3 CLI configuration, you need to issue the **commit** command before saving the configuration to flash)
- Set OVS commands
- Set CrossFlow commands

You can use either one of the following two methods to save your configuration, using the **save_config** command or the **copy running-config startup-config** command:

- Method 1: Under Linux bash, issue the following command manually (When setting OVS commands, you can only use this command to save the configuration file):

```
admin@Xorplus$ sudo save_config
```

- Method 2: In the L2/L3 CLI operating mode, issue the following command manually:

```
admin@Xorplus> copy running-config startup-config
```

Example

- Save the running configuration file from the RAM to the flash after setting the L2 / L3 CLI commands.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable true
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2
admin@Xorplus# commit
Merging the configuration.
Commit OK.
Save done.
admin@Xorplus# quit
admin@Xorplus> copy running-config startup-config
```

set cli idle-timeout

To set the maximum idle time before the current session is terminated, use the **set cli idle-timeout** command in L2/L3 operation mode.

Command Syntax

set cli idle-timeout *time*

Parameters

time	The maximum idle time before the terminal session is terminated. The range is from 0 to 2,000,000 seconds.

Examples

This example demonstrates how to set the maximum idle time to 900 seconds (15 minutes):

```
admin@Switch> set cli idle-timeout 900
```

set cli screen-length

To set the number of lines of output to display on the terminal screen for the current session before pausing, use the **set cli screen-length** command in L2/L3 operation mode.

Command Syntax

set cli screen-length *lines*

Parameters

lines	Number of lines to display. The range is from 0 to 10,000. Use 0 to not pause while displaying output.

Examples

This example shows how to set the number of lines of command output to display on the terminal before pausing:

```
admin@Switch> set cli screen-length 25
```

set cli terminal

To specify the type of terminal for the current session, use the **set cli terminal** command in L2/L3 operation mode.

Command Syntax

set cli terminal { **ansi** | **linux** | **vt100** | **xterm** }

Examples

This example shows how to set the terminal type to **linux** for the current session:

```
admin@Switch> set cli terminal linux
```

syslog monitor

The **syslog monitor** command configures whether to enable or disable the syslog monitor function.

Command Syntax

syslog monitor <**on** | **off**>

Parameter

Parameter	Description
on | off	Enable or disable the syslog monitor function. The value could be **on** or **off**. • **on**: enables the syslog monitor function. • **off**: disables the syslog monitor function. The default value is **off**.

Usage Guidelines

By configuring the syslog monitor function, you can view system log information on the user terminal (including host from which you log in to the device through the console interface) to monitor the running status of the device.

NOTE:

You can configure this command either in Linux shell or CLI mode as shown below:

- From the "**>**" prompt, use the following format,

  admin@Xorplus> syslog monitor on
- From the "**#**" prompt, use the following format,

  admin@Xorplus# run syslog monitor on

Example

- Enable the syslog monitor function.

```
admin@Xorplus> syslog monitor on
```

- Disable the syslog monitor function.

```
admin@Xorplus> syslog monitor off
```

syslog notify

The **syslog notify** command configures whether to enable or disable the function of multi-window command configuration display on the user terminal.

Command Syntax

syslog notify <**on | off**>

Parameter

Parameter	Description
on | off	Enable or disable multi-window command configuration display on the user terminal. The value is **on** or **off**. **on**: enables command configuration display on the user terminal. **off**: disables command configuration display on the user terminal. The default value is **on**.

Usage Guidelines

The CLI window will not synchronously print the configurations of the same switch from other CLI windows to the current CLI interface if disables the function of multi-window command configuration on the user terminal.

The function is window dependent, that is, it will take effect based on CLI windows regardless of the CLI login method (Console or SSH) or the login IP of terminal or the login users.

When the window is restarted, the configuration of multi-window command configuration display on the user terminal function will go to the default value.

NOTE:

You can configure this command either in Linux shell or CLI mode as shown below:

- From the ">" prompt, use the following format,

  admin@Xorplus> syslog notify on
- From the "#" prompt, use the following format,

  admin@Xorplus# run syslog notify on

Example

- Enable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify on
```

- Disable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify off
```

hwclock

hwclock is an administration tool for the time clocks. It can display the Hardware Clock time and set the Hardware Clock. Run the command with *sudo* before it, or by *root* user, as it can be executed only by the superuser.

Command Syntax

Under Linux bash, use the following format,

hwclock [*function*] [*option...*]

Parameter

Parameter	Description
function:	
-h, --help	Show help text and exit.
-r, --show	Read hardware clock and print result.
--set	Set the RTC to the time given with –date.
-s, --hctosys	Set the system time from the hardware clock.
-w, --systohc	Set the hardware clock from the current system time.
--systz	Set the system time based on the current timezone.
--adjust	Adjust the RTC to account for systematic drift since the clock was last set or adjusted.
--getepoch	Print out the kernel's hardware clock epoch value.
--setepoch	Set the kernel's hardware clock epoch value to the value given with –epoch.
--predict	Predict RTC reading at time given with –date.
-V, --version	Display version information and exit.
*option***:**	
-u, --utc	The hardware clock is kept in UTC.
--localtime	The hardware clock is kept in local time.
-f, --rtc <file>	Special /dev/... file to use instead of default.
--directisa	Access the ISA bus directly instead of /dev/rtc.
--badyear	Ignore RTC's year because the BIOS is broken.
--date <time>	Specifies the time to set the hardware clock to.
--epoch <year>	Specifies the year which is the beginning of the hardware clock's epoch value.
--noadjfile	Do not access /etc/adjtime; this requires the use of either --utc or –localtime.
--adjfile <file>	Specifies the path to the adjust file; the default is /etc/adjtime.
--test	Do not update anything, just show what would happen.
-D, --debug	Debugging mode.

Example

- Show the help information of hwclock command.

```
admin@193:/$ sudo hwclock -h
Usage:
 hwclock [function] [option...]

Functions:
 -h, --help           show this help text and exit
 -r, --show           read hardware clock and print result
     --set            set the RTC to the time given with --date
 -s, --hctosys        set the system time from the hardware clock
```

```
 -w, --systohc        set the hardware clock from the current system time
     --systz          set the system time based on the current timezone
     --adjust         adjust the RTC to account for systematic drift since
                        the clock was last set or adjusted
     --getepoch       print out the kernel's hardware clock epoch value
     --setepoch       set the kernel's hardware clock epoch value to the
                        value given with --epoch
     --predict        predict RTC reading at time given with --date
 -V, --version        display version information and exit

Options:
 -u, --utc            the hardware clock is kept in UTC
     --localtime      the hardware clock is kept in local time
 -f, --rtc <file>     special /dev/... file to use instead of default
     --directisa      access the ISA bus directly instead of /dev/rtc
     --badyear        ignore RTC's year because the BIOS is broken
     --date <time>    specifies the time to which to set the hardware clock
     --epoch <year>   specifies the year which is the beginning of the
                        hardware clock's epoch value
     --noadjfile      do not access /etc/adjtime; this requires the use of
                        either --utc or --localtime
     --adjfile <file> specifies the path to the adjust file;
                        the default is /etc/adjtime
     --test           do not update anything, just show what would happen
 -D, --debug          debugging mode
```

- Display hardware clock time.

```
admin@193:/$ sudo hwclock --show
Thu Jan 11 21:51:15 2001  -0.719120 seconds
```

rollback

The **rollback** command can be used to rollback the configuration.

Command Syntax

rollback <0 | 1 | 2 |3 | 4 | 5 | default>

Usage Guidelines

Each time a configuration in L2/L3 is commited, a rollback configuration file is created. For example, if configuration is committed five times, **pica.conf.01** through **pica.conf.05** are created. User can rollback to any of these configurations when necessary. The maximum quantity of rollback files is limited to five. The current configuration is located in ***pica.conf***. “rollback 0" refers to load the configurations in file ***pica.conf.***

The **rollback default** command completely replaces the running configuration with the default configuration file. After this command is executed, a commit is required to make the rollback to default configuration take effect.

Warning: This command should be used with caution. All the user configurations will be overridden by the default configurations.

Example

- Rollback the configuration to in configuration file **pica.conf.01**.

```
admin@XorPlus# rollback 1
admin@XorPlus# Loading config file...
Config file was loaded successfully.
admin@XorPlus# commit
Commit OK.
Save done.
```

System Management Commands

- NAC Configuration Commands
  - set protocols dot1x aaa radius authentication server-ip
  - set protocols dot1x aaa radius authentication server-ip priority
  - set protocols dot1x aaa radius authentication server-ip retry-num
  - set protocols dot1x aaa radius authentication server-ip retry-interval
  - set protocols dot1x aaa radius authentication server-ip detect-interval
  - set protocols dot1x interface auth-mode 802.1x
  - set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
  - set protocols dot1x interface auth-mode mac-radius
  - set protocols dot1x interface auth-mode web
  - set protocols dot1x interface authentication-open disable
  - set protocols dot1x aaa radius dynamic-author client
  - set protocols dot1x aaa radius dynamic-author client shared-key
  - set protocols dot1x aaa radius nas-ip
  - set protocols dot1x aaa radius accounting disable
  - set protocols dot1x interface host-mode
  - set protocols dot1x block-vlan-id
  - set protocols dot1x server-fail-vlan-id
  - set protocols dot1x filter sequence from destination-address-ipv4
  - set protocols dot1x filter sequence from destination-address-ipv6
  - set protocols dot1x filter sequence from destination-port
  - set protocols dot1x filter sequence from ether-type
  - set protocols dot1x filter sequence from source-address-ipv4
  - set protocols dot1x filter sequence from source-address-ipv6
  - set protocols dot1x filter sequence from source-port
  - set protocols dot1x filter sequence from protocol
  - set protocols dot1x filter sequence then action
  - run show dot1x all
  - run show dot1x interface
  - run show dot1x server
  - run show dot1x dynamic filter
  - run show dot1x downloadable filter
  - run show dot1x interface statistics gigabit-ethernet
  - set protocols dot1x server-fail recovery-method
  - set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
  - set protocols dot1x aaa vrf mgmt-vrf
  - set protocols dot1x interface session-timeout
  - set protocols dot1x interface recovery-timeout
  - set protocols dot1x server-fail recovery-timeout
  - set protocols dot1x interface max-sessions
  - set protocols dot1x max-sessions-per-port
  - set protocols dot1x aaa radius authentication server-ip auth-port
  - set protocols dot1x aaa radius authentication server-ip acct-port
  - set protocols dot1x aaa radius dynamic-author client port
  - run show dot1x radius-port
  - set protocols dot1x filter sequence from destination-mac-address
  - set protocols dot1x filter sequence from vlan
- SNMP Configuration Commands
  - set protocols snmp trap-group targets security-name
  - set protocols lldp snmp-trap
  - set protocols snmp trap-group event cpu-threshold enable
  - set protocols snmp trap-group event cpu-threshold high
  - set protocols snmp trap-group event cpu-threshold interval
  - set protocols snmp trap-group event cpu-threshold low
  - set protocols snmp trap-group event mac-threshold enable
  - set protocols snmp trap-group event mac-threshold interval
  - set protocols snmp trap-group event mac-threshold limit
  - set protocols snmp trap-group vrf mgmt-vrf
  - set protocols snmp trap-group version
  - set protocols snmp v3 enable
  - set protocols snmp v3 usm-user
  - set protocols snmp v3 usm-user group
  - set protocols snmp v3 group notify-view
  - set protocols snmp v3 group read-view

    - set protocols snmp v3 group write-view
    - set protocols snmp v3 group security-level
    - set protocols snmp v3 usm-user authentication-mode
    - set protocols snmp v3 usm-user authentication-key
    - set protocols snmp v3 usm-user privacy-mode
    - set protocols snmp v3 usm-user privacy-key
    - set protocols snmp v3 mib-view subtree mask
    - set protocols snmp v3 mib-view subtree type
    - set protocols snmp trap-group source-interface
    - set protocols snmp community
    - set protocols snmp community authorization
    - set protocols snmp community clients
    - set protocols snmp contact
    - set protocols snmp location
    - run show snmp statistics
- Mirror Configuration Commands
    - set interface ethernet-switching-options analyzer input
    - set interface ethernet-switching-options analyzer output
    - set interface ethernet-switching-options analyzer erspan input
    - set interface ethernet-switching-options analyzer erspan output source-ip
    - set interface ethernet-switching-options analyzer erspan output dest-ip
    - set interface ethernet-switching-options analyzer erspan output vrf
    - run show analyzer
    - set firewall filter sequence then erspan source-ip
    - set firewall filter sequence then erspan dest-ip
    - set firewall filter sequence then erspan vrf
    - set firewall filter sequence then erspan ttl
- RMON Commands
    - run show rmon alarms
    - run show rmon eventlog
    - run show rmon events
    - run show rmon history
    - run show rmon statistics
    - set protocols snmp rmon alarm falling-event-index
    - set protocols snmp rmon alarm falling-threshold
    - set protocols snmp rmon alarm interval
    - set protocols snmp rmon alarm owner
    - set protocols snmp rmon alarm rising-event-index
    - set protocols snmp rmon alarm rising-threshold
    - set protocols snmp rmon alarm sample-type
    - set protocols snmp rmon alarm variable
    - set protocols snmp rmon event community
    - set protocols snmp rmon event description
    - set protocols snmp rmon event owner
    - set protocols snmp rmon event type
    - set protocols snmp rmon history buckets
    - set protocols snmp rmon history interface
    - set protocols snmp rmon history interval
    - set protocols snmp rmon history owner
    - set protocols snmp rmon statistics interface
    - set protocols snmp rmon statistics owner
- RESTCONF Commands
    - set protocols restconf
    - set protocols restconf port
    - set protocols restconf traceoptions flag config disable
    - set protocols restconf traceoptions flag all disable
    - set protocols restconf traceoptions flag datastore disable
- run show system boot-messages
- run show system connections
- run show system core-dumps
- run show system cpu-usage
- run show system date
- run show system fan
- run show system memory-usage
- run show system name
- run show system ntp-status
- run show system os
- run show system processes brief
- run show system processes detail
- run show system rollback compare to
- run show system rollback file

- run show system rollback list
- run show system rpsu
- run show system serial-number
- run show system temperature
- run show system uptime
- run show system users
- set system aaa local disable
- set system aaa radius accounting disable
- set system aaa radius accounting server-ip
- set system aaa radius accounting server-ip port
- set system aaa radius accounting server-ip shared-key
- set system aaa radius accounting server-ip timeout
- set system aaa radius authorization disable
- set system aaa radius authorization server-ip
- set system aaa radius authorization server-ip port
- set system aaa radius authorization server-ip shared-key
- set system aaa radius authorization server-ip timeout
- set system aaa radius vrf mgmt-vrf
- set system aaa tacacs-plus accounting
- set system aaa tacacs-plus authorization
- set system aaa tacacs-plus auth-type
- set system aaa tacacs-plus disable
- set system aaa tacacs-plus key
- set system aaa tacacs-plus port-number
- set system aaa tacacs-plus timeout
- set system aaa tacacs-plus server-ip
- set system aaa tacacs-plus source-interface
- set system aaa local-auth-fallback disable
- set system aaa tacacs-plus vrf mgmt-vrf
- set system hostname
- set system inband vlan-interface
- set system inband loopback
- set system inband routed-interface
- set system inband enable
- system login-acl network
- system login announcement
- system login user
- system login user admin class
- set system login user authentication plain-text-password
- system login user class
- set system timezone
- set system ntp server-ip
- set system ntp source-interface
- set system ntp vrf mgmt-vrf
- set interface gigabit-ethernet ptp mode
- set system services ssh connection-limit
- set system services ssh disable
- set system services ssh protocol-version v2
- set system services ssh rate-limit
- set system services ssh root-login
- set system services ssh idle-timeout
- set system services ssh port
- set system snmp-acl security-name network
- set system syslog server-ip
- set system syslog local-file
- set system syslog vrf mgmt-vrf
- set system usb disable
- set system management-ethernet eth0 ip-address {IPv4 | IPv6}
- set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}
- show system management-ethernet
- run request system reboot
- run show system hwinfo
- ping
- traceroute
- tftp
- set protocols sflow collector vrf mgmt-vrf
- scp
- set system login banner
- upgrade2 image-file
- upgrade2 image-file backup-file

- upgrade2 image-file factory-default
- upgrade2 image-file use-prev-config
- set system dns-server-ip
- set system console idle-timeout
- set system login multiline-banner message
- set system login multiline-announcement message
- set system aaa radius source-interface
- set protocols grpc enable
- set protocols grpc port
- set system ztp enable
- telnet
- set system start-shell-sh password
- set system services telnet disable
- set system services web disable

NAC Configuration Commands

- set protocols dot1x aaa radius authentication server-ip
- set protocols dot1x aaa radius authentication server-ip priority
- set protocols dot1x aaa radius authentication server-ip retry-num
- set protocols dot1x aaa radius authentication server-ip retry-interval
- set protocols dot1x aaa radius authentication server-ip detect-interval
- set protocols dot1x interface auth-mode 802.1x
- set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
- set protocols dot1x interface auth-mode mac-radius
- set protocols dot1x interface auth-mode web
- set protocols dot1x interface authentication-open disable
- set protocols dot1x aaa radius dynamic-author client
- set protocols dot1x aaa radius dynamic-author client shared-key
- set protocols dot1x aaa radius nas-ip
- set protocols dot1x aaa radius accounting disable
- set protocols dot1x interface host-mode
- set protocols dot1x block-vlan-id
- set protocols dot1x server-fail-vlan-id
- set protocols dot1x filter sequence from destination-address-ipv4
- set protocols dot1x filter sequence from destination-address-ipv6
- set protocols dot1x filter sequence from destination-port
- set protocols dot1x filter sequence from ether-type
- set protocols dot1x filter sequence from source-address-ipv4
- set protocols dot1x filter sequence from source-address-ipv6
- set protocols dot1x filter sequence from source-port
- set protocols dot1x filter sequence from protocol
- set protocols dot1x filter sequence then action
- run show dot1x all
- run show dot1x interface
- run show dot1x server
- run show dot1x dynamic filter
- run show dot1x downloadable filter
- run show dot1x interface statistics gigabit-ethernet
- set protocols dot1x server-fail recovery-method
- set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
- set protocols dot1x aaa vrf mgmt-vrf
- set protocols dot1x interface session-timeout
- set protocols dot1x interface recovery-timeout
- set protocols dot1x server-fail recovery-timeout
- set protocols dot1x interface max-sessions
- set protocols dot1x max-sessions-per-port
- set protocols dot1x aaa radius authentication server-ip auth-port
- set protocols dot1x aaa radius authentication server-ip acct-port
- set protocols dot1x aaa radius dynamic-author client port
- run show dot1x radius-port
- set protocols dot1x filter sequence from destination-mac-address
- set protocols dot1x filter sequence from vlan

set protocols dot1x aaa radius authentication server-ip

The **set protocols dot1x aaa radius authentication server-ip** command configures the IP address and shared key of the RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **shared-key** <*key-string*>

Parameter

Parameter	Description
server-ip <*ip-address*>	Specifies IPv4 address of RADIUS authentication server.
shared-key <*key-string*>	Specifies the shared key of RADIUS authentication server. The value is a string type. Note: The value of shared key should be the same as that on the RADIUS authentication server.

Usage Guidelines

The AAA RADIUS authentication server is used in NAC authentication, including 802.1X authentication, MAB authentication, CWA authentication, Downloadable ACL and Dynamic ACL functions, exchanges RADIUS packet with the switch. Note that up to 20 AAA RADIUS servers can be configured on the switch. The server with the smallest IP address and reachable is used for NAC authentication.

Example

- Configure the IP address and shared key of the 802.1X RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 shared-key pica8abc
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip priority

The **set protocols dot1x aaa radius authentication server-ip** priority command configures the priority of the AAA RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **priority** <*priority*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
priority <*priority*>	Specifies the priority of RADIUS authentication server. The value is an integer that ranges from 1 to 20. Priority of 1 is higher than 20. If the priority is not specified for a AAA server, the default priority is infinity, indicating a lowest priority.

Usage Guidelines

Note: Up to 20 AAA RADIUS servers can be configured on the switch.

If several AAA RADIUS servers have been deployed, users can specify different priority for different server by using this command. AAA RADIUS server with higher priority is selected for NAC authentication.

If two servers have the same priority, the server with the smallest IP address and reachable will be used for NAC authentication.

Example

- Configure the priority of the AAA RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 priority 2
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip retry-num

The **set protocols dot1x aaa radius authentication server-ip retry-num** command configures the maximum number of authentication attempts when the AAA server does not respond during NAC authentication.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **retry-num** <*retry-num*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
retry-num <*retry-num*>	Specifies the maximum number of authentication attempts. The value is an integer that ranges from 1 to 5. The default value is 3.

Usage Guidelines

When performing NAC authentication, if the AAA server does not respond to the switch, switch sends authentication message to the AAA server for several times. Use this command to configure the maximum number of authentication attempts, use another command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-interval** <*retry-interval*> to configure the interval for re-sending the authentication messages.

If the AAA server still does not respond after trying the times of **retry-num**, the AAA server is considered inaccessible. If all the AAA servers are inaccessible, the access port of the client will be added to the server fail VLAN, and the packets from the client can only be forwarded in this VLAN.

Example

- Configure the maximum number of authentication attempts to 2.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 retry-num 2
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip retry-interval

The **set protocols dot1x aaa radius authentication server-ip retry-interval** command configures the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond during NAC authentication.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **retry-interval** <*retry-interval*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
retry-interval <*retry-interval*>	Specifies the interval for re-sending the authentication messages. The value is an integer that ranges from 1 to 5, in seconds. The default value is 1s.

Usage Guidelines

When performing NAC authentication, if the AAA server does not respond to the switch, switch re-sends authentication message to the AAA server for several times. Use command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-num** <*retry-num*> to configure the maximum number of authentication attempts, use command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-interval** <*retry-interval*> to configure the interval for re-sending the authentication messages.

If the AAA server still does not respond after trying the times of **retry-num**, it is considered inaccessible. If all the AAA servers are inaccessible, the access port of the client will be added to the server fail VLAN, and the packets from the client can only be forwarded in this VLAN.

Example

- Configure the interval for re-sending the authentication messages.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 retry-interval 3
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip detect-interval

The **set protocols dot1x aaa radius authentication server-ip detect-interval** command configures the detection interval of the AAA RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **detect-interval** <*detect-interval*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
detect-interval <*detect-interval*>	Specifies the detection interval. The value is an integer that ranges from 0 to 300, in seconds, where “0” indicates disabling detect function. The default value is 5s.

Usage Guidelines

After a AAA server is configured, the switch sends Test Radius Request detection message to the server to detect the reachability of the AAA server. If the AAA server is not reachable, switch will re-send the Test Radius Request message again after the detection interval to detect the reachability of the AAA server until the AAA server is reachable.

Example

- Configure the detection interval of the AAA RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 detect-interval 10
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode 802.1x

The **set protocols dot1x interface auth-mode 802.1x** command enables the 802.1X authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI command **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI command **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

802.1X authentication is an authentication method that controls the network access rights of users based on ports together with the MAC address of client. The Extensible Authentication Protocol (EAP) packet is used to exchange authentication information between the supplicant, authenticator and authentication server. This technology is mainly used in networks with high security requirements. 802.1X authentication requires 802.1X client software to be installed on the supplicant.

Example

- Enable 802.1X authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode 802.1x fallback-to-web disable

The **set protocols dot1x interface auth-mode 802.1x fallback-to-web disable** command enables or disables fallback to WEB function.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x fallback-to-web disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
disable <**true**	**false**>	Enables or disables fallback to WEB function. The value could be **true** or **false**. • **true:** disables fallback to WEB function. • **false:** enables fallback to WEB function. By default, fallback to WEB function is disabled.

Example

- Enable fallback to WEB function on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x fallback-to-web disable false
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode mac-radius

The **set protocols dot1x interface auth-mode mac-radius** command enables the MAB authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode mac-radius**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI node **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI node **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

During the MAB authentication process, the user is not required to manually enter a username or password. The user's MAC address will be encapsulated as user name and password in the packet and sent to the RADIUS server. The port will be opened to the user with this MAC only if it passes the MAB authentication. This technology is suitable for environments where the MAC address is fixed and the security requirements are not very high. At the same time, it can meet the authentication requirements of terminals such as printers that cannot install the authentication client software.

When both 802.1X authentication and MAB authentication modes are enabled, the 802.1X authentication will take precedence over MAB. If the Supplicant supports 802.1x authentication, the system performs 802.1x authentication. Else if the Supplicant does not support 802.1x authentication, the system performs MAB authentication. For the former case, no matter whether 802.1x authentication is successful or not, the MAB authentication process will not be taken.

Example

- Enable MAB authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode web

The **set protocols dot1x interface auth-mode web** command enables the Web authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode web**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI command **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI command **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

Example

- Enable Web authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode web
admin@Xorplus# commit
```

set protocols dot1x interface authentication-open disable

The **set protocols dot1x interface authentication-open disable** command enables open authentication function on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **authentication-open disable <true | false>**

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
disable <true | false>	Configures whether to enable or disable the open authentication function. The value is **true** or **false**. • **true**: disables the open authentication function. • **false**: enables the open authentication function. The default value is **true**.

Usage Guidelines

With open authentication function, only DHCP packets are allowed on the specified port to make Client could get IP address before any authentication has succeeded.

Example

- Enable the open authentication function on ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 authentication-open disable false
```

set protocols dot1x aaa radius dynamic-author client

The **set protocols dot1x aaa radius dynamic-author client** command configures IP address of the RADIUS dynamic authorization client (DAC) for Change of Authorization (CoA) function.

RADIUS dynamic authorization client could be the same RADIUIS authentication server configured in **set protocols dot1x aaa radius authentication server-ip** *<ip-address>* [**shared-key** *<key-string>*] command or it could be a different one.

> **NOTE:**
>
> PICOS supports to configure a maximum of 20 CoA dynamic authorization clients.

Command Syntax

set protocols dot1x aaa radius dynamic-author client *<client-ip>*

Parameter

Parameter	Description
client *<client-ip>*	Specifies the IP address of the RADIUS dynamic authorization client. This component often resides on the RADIUS server.

Example

- Configure the client for CoA function.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1
admin@Xorplus# commit
```

set protocols dot1x aaa radius dynamic-author client shared-key

The **set protocols dot1x aaa radius dynamic-author client shared-key** command configures the IP address and the shared key of the RADIUS dynamic authorization client (DAC) for Change of Authorization (CoA) function.

> **NOTE:**
>
> This command is supported from PICOS 2.11.16.

Command Syntax

set protocols dot1x aaa radius dynamic-author client <*client-ip*> **shared-key** <*key-string*>

Parameter

Parameter	Description
client <*client-ip*>	Specifies the IP address of the RADIUS dynamic authorization client. This component often resides on the RADIUS authentication server.
shared-key <*key-string*>	Specifies the shared key of the RADIUS dynamic authorization client. The value is a string type. Note: The value of shared key should be the same as the one configured on the RADIUS dynamic authorization client.

Example

- Configure the IP address and the shared key of the RADIUS dynamic authorization client.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1 shared-key pica8123
admin@Xorplus# commit
```

set protocols dot1x aaa radius nas-ip

The **set protocols dot1x aaa radius nas-ip** command configures the NAS IP address to the interface IP which connected to the RADIUS server.

Command Syntax

set protocols dot1x aaa radius nas-ip <*ip-address*>

Parameter

Parameter	Description
nas-ip <*ip-address*>	Specifies the NAS IP address to the interface IP which connected to the RADIUS server.

Usage Guidelines

This command is to set the nas-ip field in RADIUS access-request message. The value of the NAS IP address depends on the port connected to the RADIUS authentication server:

- If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.
- If you use the L3 VLAN interface, loopback interface, routed interface or sub-interface to connect to the RADIUS server, the IP address of the L3 VLAN interface, loopback interface, routed interface or sub-interface should be used for the NAS IP address configured here.

Example

- Configure the NAS IP address to the interface IP which connected to the RADIUS server.

```
admin@Xorplus# set protocols dot1x aaa radius nas-ip 10.10.10.100
admin@Xorplus# commit
```

set protocols dot1x aaa radius accounting disable

The **set protocols dot1x aaa radius accounting disable** command enables or disables user accounting function when performing NAC authentication.

NOTE:

RADIUS accounting applies only to 802.1X and MAB authentication procedures.

Command Syntax

set protocols dot1x aaa radius accounting disable <**true | false**>

Parameter

Parameter	Description
disable <**true	false**>	Enables or disables user accounting function when performing NAC authentication. The value could be **true** or **false**. • **true:** disables user accounting function. • **false:** enables user accounting function. By default, user accounting function is enabled.

Example

- Enable user accounting function when performing NAC authentication.

```
admin@Xorplus# set protocols dot1x aaa radius accounting disable false
admin@Xorplus# commit
```

set protocols dot1x interface host-mode

The **set protocols dot1x interface host-mode** command configures host access mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **host-mode** <**single** | **multiple**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
host-mode <**single** | **multiple**>	Specifies host access mode. The value could be **single** or **multiple**. • **Single:** Only one user is allowed to access the switch port, unless the user goes offline other users cannot try to access the port. The authentication will be restarted if port is bounced or client is changed. • **Multiple:** T Multiple clients connect to the network through the same switch port. If a user goes offline, the network access rights of other users are not affected. At most 8 clients are allowed to be authenticated on a single switch port, the ninth will be added into the pending list. The default host mode is **single**. Note that changing host mode from CLI will cause re-authentication for all online users of the port.

Usage Guidelines

This command is to set the nas-ip field in RADIUS access-request message. The value of the NAS IP address depends on the port connected to the RADIUS authentication server:

- If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.
- If you use the L3 VLAN interface to connect to the RADIUS server, the IP address of the L3 VLAN interface should be used for the NAS IP address configured here.

Example

- Configure the host access mode as multiple on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 host-mode multiple
admin@Xorplus# commit
```

set protocols dot1x block-vlan-id

The **set protocols dot1x block-vlan-id** command configures block VLAN ID.

Command Syntax

set protocols dot1x block-vlan-id <*vlan-id*>

Parameter

Parameter	Description
block-vlan-id <*vlan-id*>	Specifies the VLAN ID for block VLAN. The value is an integer that ranges from 2 to 4094.

Example

- Configure the block VLAN ID to 100.

```
admin@Xorplus# set protocols dot1x block-vlan-id 100
admin@Xorplus# commit
```

set protocols dot1x server-fail-vlan-id

The **set protocols dot1x server-fail-vlan-id** command configures a server fail VLAN.

Command Syntax

set protocols dot1x server-fail-vlan-id <*vlan-id*>

Parameter

Parameter	Description
server-fail-vlan-id <*vlan-id*>	Specifies the VLAN ID for a server fail VLAN. The value is an integer that ranges from 2 to 4094.

Example

- Configure the server fail VLAN ID to 200.

```
admin@Xorplus# set protocols dot1x server-fail-vlan-id 200
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-address-ipv4

The **set protocols dot1x filter sequence from destination-address-ipv4** command configures the destination IPv4 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-address-ipv4 <*ipv4-address*>	Specifies the destination IPv4 address of packets that match ACL rules. It must be an IPv4 subnet in address/prefix-length form. For example, 10.1.1.0/24.

Example

- Configure the destination IPv4 address of packets that match ACL rules to 10.1.1.0/24.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-address-ipv4 10.1.1.0/24
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-address-ipv6

The **set protocols dot1x filter sequence from destination-address-ipv6** command configures the destination IPv6 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-address-ipv6 <*ipv6-address*>	Specifies the destination IPv6 address of packets that match ACL rules. It must be an IPv6 subnet in address/prefix-length form. For example, 10::1/128.

Example

- Configure the destination IPv6 address of packets that match ACL rules to 10::1/128.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-address-ipv6 10::1/128
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-port

The **set protocols dot1x filter sequence from destination-port** command configures the destination port information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-port** <*port-number*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-port <*port-number*>	Specifies the destination port of packets that match ACL rules. The value is an integer. It could be a port number or a range of port number, i.e. 6000; 6000..7000, which indicates port range from 6000 to 7000.

Example

- Configure the destination port of packets that match ACL rules to 6000.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-port 6000
admin@Xorplus# commit
```

set protocols dot1x filter sequence from ether-type

The **set protocols dot1x filter sequence from ether-type** command configures the Ethernet type information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter *<filter-name>* **sequence** *<sequence-number>* **from ether-type** *<ether-type>*

Parameter

Parameter	Description
filter *<filter-name>*	Specifies the ACL filter name. The value is a string.
sequence *<sequence-number>*	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
ether-type *<ether-type>*	Specifies the Ethernet type of packets that match ACL rules. The value is an integer in decimal format that ranges from 1501 to 65535.

Example

- Configure the Ethernet type of packets that match ACL rules to 4525.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from ether-type 4525
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-address-ipv4

The **set protocols dot1x filter sequence from source-address-ipv4** command configures the source IPv4 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from source-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-address-ipv4 <*ipv4-address*>	Specifies the source IPv4 address of packets that match ACL rules. It must be an IPv4 subnet in address/prefix-length form. For example, 10.1.1.0/24.

Example

- Configure the source IPv4 address of packets that match ACL rules to 172.1.1.0/24.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-address-ipv4 172.1.1.0/24
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-address-ipv6

The **set protocols dot1x filter sequence from source-address-ipv6** command configures the source IPv6 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from source-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-address-ipv6 <*ipv6-address*>	Specifies the source IPv6 address of packets that match ACL rules. It must be an IPv6 subnet in address/prefix-length form. For example, 0a::1/128.

Example

- Configure the source IPv6 address of packets that match ACL rules to 0a::1/128.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-address-ipv6 0a::1/128
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-port

The **set protocols dot1x filter sequence from source-port** command configures the source port information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter *<filter-name>* **sequence** *<sequence-number>* **from *source-port*** *<port-number>*

Parameter

Parameter	Description
filter *<filter-name>*	Specifies the ACL filter name. The value is a string.
sequence *<sequence-number>*	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-port *<port-number>*	Specifies the source port of packets that match ACL rules. The value is an integer. It could be a port number or a range of port number, i.e. 6000; 6000..7000, which indicates port range from 6000 to 7000.

Example

- Configure the source port of packets that match ACL rules to 7000.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-port 7000
admin@Xorplus# commit
```

set protocols dot1x filter sequence from protocol

The **set protocols dot1x filter sequence from protocol** command configures the protocol type information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from protocol [icmp | igmp | ip | ospf | others**<*protocol-number*> **| udp | tcp]**

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
protocol [icmp | igmp | ip | ospf | others <*protocol-number***> | udp | tcp]**	Specifies a protocol name or a protocol number. • Protocol name could be **icmp, igmp, ip, ospf, udp** or **tcp**. • Protocol number is an integer that ranges from 0 to 255. For example, 8 for EGP, 9 for IGP, 47 for GRE, 88 for EIGRP, 103 for PIM, and 112 for VRRP.

Example

- Configure the protocol type of packets that match ACL rules to ICMP.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from protocol icmp
admin@Xorplus# commit
```

set protocols dot1x filter sequence then action

The **set protocols dot1x filter sequence then action** command configures the action for packets that match the ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **then action** <**discard** | **forward**>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
action <**discard** | **forward**>	Specifies the action for packets that match the ACL rules. The value could be **discard** or **forward**. • **discard:** Discard packets that match all match conditions in the same sequence number. • **forward:** Forward packets that match all match conditions in the same sequence number.

Example

- Configure the action for packets that match the ACL rules to discard.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 then discard
admin@Xorplus# commit
```

run show dot1x all

The **run show dot1x all** command displays the NAC information.

Command Syntax

run show dot1x all

Parameter

None.

Example

- Run **run show dot1x all** command to view the NAC information.

```
admin@Xorplus# run show dot1x all
Global-Info:
--------------------------------------------------------------------------------
NAS-IP              :  10.10.1.1
Block-VLAN         :  2
Block-VLAN-IP       :  172.16.1.1/24
WEB-AUTH-MODE   :  Remote
Server-Fail-VLAN           :  100
--------------------------------------------------------------------------------
```

Table 1 Description of the **run show dot1x all** command output

Item	Description
NAS-IP	Indicates the NAS IP address which is set to the L3 VLAN interface IP connected to the RADIUS server.
Block-VLAN	Indicates the VLAN ID for block VLAN.
Block-VLAN-IP	Indicates the IP address of the L3 block VLAN interface.
WEB-AUTH-MODE	Indicates the Web authentication mode, the value is **Remote**.
Server-Fail-VLAN	Indicates the VLAN to which the user ports will be added to when all the configured RADIUS servers are unreachable.

run show dot1x interface

The **run show dot1x interface** command displays the configuration information and port status of NAC authentication function on the interface.

Command Syntax

run show dot1x interface [**gigabit-ethernet** <*interface-name*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies the physical interface name.

Usage Guidelines

You can use this command to view the NAC authentication information of the client on all the interface enabled with NAC or on a specified interface. This command can also be used to view the dynamic ACL and downloadable ACL information.

Example

- Run **run show dot1x interface gigabit-ethernet** <*interface-name*> command to view the detailed NAC information on a specified interface.

```
admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/48
Interface ge-1/1/48:
============================================================
  Client MAC                : 00:00:00:11:11:11
  Status                    : authorized
  Success Auth Method       : MAB
  Last Success Time         : Sun Mar 20 21:08:11 2022
  Traffic Class             : Other
  Downloadable Filter Name  : pica-dacl-mab (active)
============================================================

admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/13
Interface ge-1/1/13:
============================================================
  Client MAC                : 08:9e:01:9e:cc:fe
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
============================================================


admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/14
Interface ge-1/1/14:
============================================================
  Client MAC                : 00:00:00:22:55:56
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
  Downloadable Filter Name  : f1
============================================================


admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/15
Interface ge-1/1/15:
============================================================
  Client MAC                : 00:00:00:22:55:56
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
  Dynamic Filter Name       : f2(active)
```

```
============================================================
```

- Run **run show dot1x interface** command to view the brief NAC information on all the NAC enabled interfaces.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x  MAC-RADIUS  WEB  HOST-MODE  Session-Timeout  CLIENT-MAC  CLIENT-STATUS
-------------------------------------------------------------------------------------------------------------------------
ge-1/1/1  disable   enable      disable   single(0)       0    00:11:22:33:44:55   unauthorized
ge-1/1/3  disable   enable      enable    multiple(1)     0
```

Table 1. Description of the run show dot1x interface command output

Item	Description
Client MAC	Indicates the MAC address of the clients connected to the interface.
Status	Indicates the authentication status of the client. The value could be **unauthorized** or **authorized**.
Success Auth Method	Indicates the authentication method used when the authentication status is authorized. The value could be **Dot1x** or **MAB**.
Redirect URL	Indicates the redirect URL delivered from the AAA server before Web authentication succeeds.
Dynamic VLAN ID	Indicates the dynamic VLAN ID delivered from the RADIUS authentication server. The active or inactive in parentheses indicates whether the dynamic VLAN is configured on the switch.
Downloadable Filter Name	Displays the downloadable filter name that is delivered to the client. Users can use command **run show dot1x downloadable filter** [<*filter-name*>] to display the details of downloadable filter rule.
Dynamic Filter Name	Displays the dynamic filter name that is delivered to the client. The active or inactive in parentheses indicates whether the dynamic filter is configured on the switch.
Interface	Indicates the physical interfaces enabled NAC.
802.1x	Indicates whether the 802.1X authentication is enabled. • **enable**: indicates the 802.1X authentication is enabled. • **disable**: indicates the 802.1X authentication is disabled.
MAC-RADIUS	Indicates whether the MAB authentication is enabled. • **enable**: indicates the MAB authentication is enabled. • **disable**: indicates the MAB authentication is disabled.
WEB	Indicates whether the Web authentication is enabled. • **enable**: indicates the Web authentication is enabled. • **disable**: indicates the Web authentication is disabled.
HOST-MODE	Host mode of interface and the number of active sessions. The value could be **single(N)** or **multiple(N)**, where "N" is the number of active sessions. • **single(N):** Only one user is allowed to access the switch port, unless the user goes offline other users can try to access the port. The authentication will be restarted if port is bounced or client is changed. • **multiple(N):** Multiple clients connect to the network through the same switch port. If a user goes offline, the network access rights of other users are not affected. At most 8 clients are allowed to be authenticated on a single switch port, the ninth will be added into the pending list. The default host mode is **single**. Note that changing host mode from CLI will cause re-authentication for all online users of the port.
Session-Timeout	Indicates the expire timer for the authenticated session.
CLIENT-MAC	Indicates the MAC address of the clients connected to the interface.
CLIENT-STATUS	Indicates the authentication status of the client. The value could be **unauthorized** or **authorized**.

run show dot1x server

The **run show dot1x server** command displays the reachability of the AAA servers configured on the switch.

Command Syntax

run show dot1x server

Parameter

None.

Example

- Run **run show dot1x server** command to view reachability of the RADIUS servers.

```
admin@Xorplus# run show dot1x server
Server-IP         Status        Priority  Retry-Interval  Retry-Num  Detect-Interval   Consecutive-Detect-Num
---------------   ------------  --------  --------------  ---------  --------------    ----------------------
10.10.53.72       reachable     ...       5   Sec(s)      5          5   Sec(s)        8
```

Table 1. Description of the run show dot1x server command output

Item	Description
Server-IP	Indicates the RADIUS Server IP configured on the switch.
Status	Indicates whether the RADIUS server is reachable. The value could be **active**, **reachable** or **unreachable**. If the server is reachable and currently selected for NAC authentication, the “Status” of this server is **active**.
Priority	Indicates the priority of AAA server. The value is an integer that ranges from 1 to 3. Priority of 1 is higher than 3. “...” indicates a lowest priority if not configured for the AAA server. Note: The AAA servers are listed in the order of priority.
Retry-Interval	Indicates the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond during NAC authentication.
Retry-Num	Indicates the maximum number of authentication attempts when the AAA server does not respond during NAC authentication.
Detect-Interval	Indicates the interval at which the switch sends Test Radius Request detection message to the AAA server to detect the server reachability.
Consecutive-Detect-Num	Indicates the number of Test Radius Request messages that the switch consecutively sends to the AAA server to detect the server reachability.

run show dot1x dynamic filter

The **run show dot1x dynamic filter** command displays the dynamic filter rules configured on the switch.

Command Syntax

run show dot1x dynamic filter *<filter-name>*

Parameter

Parameter	Description
<filter-name>	Optional. Specifies the dynamic ACL filter name. The value is a string. • If displaying with a filter name, display the specified dynamic ACL filter rules. • If displaying without a filter name, display all the configured dynamic ACL filter rules.

Exampe

- Configure the dynamic ACL rules on the switch then run **run show dot1x dynamic filter** command to view the configurations.

```
admin@Xorplus# set protocols dot1x filter f4 sequence 500 from destination-address-ipv4 192.168.2.0/24
admin@Xorplus# set protocols dot1x filter f4 sequence 500 then forward
admin@Xorplus# run show dot1x dynamic filter
==================================================================
Filter: f4
    Description :
    ------------------------------------------------------------------
    Sequence            : 500
        Description      :
        Match counter    :  60544 packets
        Match Condition  :
                          Destination IPv4Net : 192.168.2.0/24
        Action          : FORWARD
==================================================================
        Applied Clients   : ge-1/1/1 00:00:00:11:22:33
```

run show dot1x downloadable filter

The **run show dot1x downloadable filter** command displays the downloadable filter rules delivered from the RADIUS authentication server.

Command Syntax

run show dot1x downloadable filter [<*filter-name*>]

Parameter

Parameter	Description
<*filter-name*>	Optional. Specifies the downloadable filter rule name.

Exampe

- Display the downloadable filter rules delivered from the RADIUS authentication server.

```
admin@Xorplus# run show dot1x downloadable filter
================================================
Filter: IP_Attendance_CTRL_Access
Description     :
------------------------------------------------------------------------
Sequence        : 1
Description     :
Match counter   : 0 packets
Match Condition : L4 Destination Port  : 67..67
                  L4 Source Port       : 68..68
                  Protocol             : udp
                  Action               : Forward
 ------------------------------------------------------------------------
Sequence        : 2
Description     :
Match counter   : 51 packets
Match Condition : L4 Destination Port  : 53..53
                  Protocol             : udp
                  Action               : Forward
------------------------------------------------------------------------
```

run show dot1x interface statistics gigabit-ethernet

The **run show dot1x interface statistics gigabit-ethernet** command displays the 802.1X statistics information on an interface.

Command Syntax

run show dot1x interface statistics gigabit-ethernet <*interface-name*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. The value is a string.

Example

- Run **run show dot1x interface statistics gigabit-ethernet** command to display the 802.1X statistics information on interface ge-1/1/1.

```
admin@Xorplus# run show dot1x interface statistics gigabit-ethernet ge-1/1/1
Interface ge-1/1/1:
================================================================================
    Client MAC : 00:11:22:33:44:55
    ----------------------------------------------------------------------
    SENT:
      EAPOL LogOff Packets : 0
      EAPOL EAP Packets    : 0
      EAP Request Packets  : 0
      EAP Response Packets : 0
      EAP Success Packets  : 0
      EAP Failure Packets  : 0
      Radius Packets       : 2
    ----------------------------------------------------------------------
    RECEIVED:
      EAPOL Start Packets  : 0
      EAPOL LogOff Packets : 0
      EAPOL EAP Packets    : 0
      EAP Request Packets  : 0
      EAP Response Packets : 0
      EAP Success Packets  : 0
      EAP Failure Packets  : 0
      Radius Packets       : 1
```

set protocols dot1x server-fail recovery-method

The **set protocols dot1x server-fail recovery-method** command configures the way to get the client port out the server fail VLAN when the server is reachable.

Command Syntax

set protocols dot1x server-fail recovery-method <auto | manual | timer >

Parameter

Parameter	Description
recovery-method <auto | manual | timer >	Specifies the way to get the client port out the server fail VLAN when the server is reachable, the value could be **auto**, **manual** or **timer**. • **auto**: The system automatically removes the client port from the server fail VLAN when the server is reachable, and take authentication again. • **manual**: Manually remove the client port from the server fail VLAN when the server is reachable. Users need to clear MAC or bounce port to trigger client to take authentication again, otherwise the client port will not be removed from the server fail VLAN when the server is reachable. • **timer**: Remove the client port from the server fail VLAN after a certain amount of time when the server is reachable. The timer can be set by command **set protocols dot1x interface recovery-timeout**. The default value is **manual**.

Usage Guidelines

If all the RADIUS servers are unreachable, the port connected to the client will be added to the server fail VLAN, and the packets from the client can be forwarded in server fail VLAN. The switch continues to send the detection packets continuously until the server is reachable. If one of the RADIUS servers is reachable, the switch removes this client from the server fail VLAN and adds it back into the block VLAN. This command configures the way to get the client port out the server fail VLAN when the server is reachable.

Example

- Configure the way to get the client port out the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x server-fail recovery-method auto
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip consecutive-detect-num

The **set protocols dot1x aaa radius authentication server-ip consecutive-detect-num** command configures the number of Test Radius Request messages that the switch consecutively sends to the AAA server to detect the server reachability.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <ipv4-address> **consecutive-detect-num** <*detect-num*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of AAA server.
consecutive-detect-num <*detect-num*>	Specifies the number of Test Radius Request message that the switch consecutively sends to the server. The value is an integer that ranges from 1 to 10. The default value is 3.

Usage Guidelines

The AAA server is considered to be reachable only when every Test Radius Request message consecutively sent by the switch receives a RADIUS access-accept message reply from the AAA server, otherwise the server is considered unreachable. The switch will continue to send the Test Radius Request message until the server is reachable.

Example

- Configure the number of Test Radius Request messages that the switch consecutively sends.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 consecutive-detect-num 5
admin@Xorplus# commit
```

set protocols dot1x aaa vrf mgmt-vrf

The **set protocols dot1x aaa vrf mgmt-vrf** command configures to run the 802.1X protocols in the management VRF.

Command Syntax

set protocols dot1x aaa vrf mgmt-vrf

Parameter

None.

Usage Guidelines

802.1X protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running 802.1X protocol.

Using this command to modify the VRF where to run the 802.1X service does not affect users who are currently authenticated successfully and online, it will only affect users who need to do DOT1X authentication later.

Note: The latest configuration overrides the previous one.

Example

- Configure the 802.1X protocols to run in the management VRF.

```
admin@Xorplus# set protocols dot1x aaa vrf mgmt-vrf
admin@Xorplus# commit
```

set protocols dot1x interface session-timeout

The **set protocols dot1x interface session-timeout** command configures the expire timer for the authenticated session.

Command Syntax

set protocols dot1x [**interface** <*interface-name*>] **session-timeout** <*session-timeout*>

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on. If no interface is specified, it represents a global configuration.
session-timeout <*session-timeout*>	Specifies the expire timer for the authenticated session. The value is an integer that ranges from 0 to 86400, in seconds. The default value is 3600s. Note that, “0” indicates authenticated session will never expire.

Usage Guidelines

The authenticated session will expire after a period of **session-timeout** and start a new authentication process. The switch will send request packet to the AAA server or the client after the expire timer for re-authentication.

The AAA server can also issue session-timeout, which takes precedence over the local configuration on the switch. About the processing for session-timeout Attribute issued by the AAA server, see section **Response to session-timeout Attribute** in Principle of NAC.

Note:

- The session timeout configuration based on an interface takes precedence over that of the global configuration.
- Configuration changes will only affect clients who need to do DOT1X authentication later.

Example

- Configure the global session expire timer for the authenticated session.

```
admin@Xorplus# set protocols dot1x session-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x interface recovery-timeout

The **set protocols dot1x interface recovery-timeout** command configures the timer after which to remove the client port from the server fail VLAN when the server is reachable.

NOTE: The **recovery-timeout** takes effect only when the recovery-method is set to “timer”.

Command Syntax

set protocols dot1x interface <*interface-name*> **recovery-timeout** <*recovery-timeout*>

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
recovery-timeout <*recovery-timeout*>	Specifies the timer after which to remove the client port from the server fail VLAN when the server is reachable. The value is an integer that ranges from 300 to 86400, in seconds. The default value is 3600 seconds.

Usage Guidelines

This command is a interface-based configuration. PICOS supports to configure the timer globally for all the switch interface after which to remove the client port from the server fail VLAN when the server is reachable by using the command set protocols dot1x server-fail recovery-timeout.

Note that the recovery timeout configuration based on an interface takes precedence over that of the global configuration.

Example

- Configure the timer after which to remove the client port from the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x recovery-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x server-fail recovery-timeout

The **set protocols dot1x server-fail recovery-timeout** command configures the timer globally after which to remove the client port from the server fail VLAN when the server is reachable.

NOTE: The **recovery-timeout** takes effect only when the recovery-method is set to “timer”.

Command Syntax

set protocols dot1x server-fail recovery-timeout *<recovery-timeout>*

Parameter

Parameter	Description
recovery-timeout *<recovery-timeout>*	Specifies the timer after which to remove the client port from the server fail VLAN when the server is reachable. The value is an integer that ranges from 300 to 86400, in seconds. The default value is 3600 seconds.

Usage Guidelines

This command is a global configuration for all the switch interface. PICOS supports to configure the timer based on an interface after which to remove the client port from the server fail VLAN when the server is reachable by using the command set protocols dot1x interface recovery-timeout.

Note that the recovery timeout configuration based on an interface takes precedence over that of the global configuration.

Example

- Configure the timer after which to remove the client port from the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x recovery-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x interface max-sessions

The **set protocols dot1x interface max-sessions** command configures the maximum number of NAC sessions that are allowed to be established on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **max-sessions** <*max-sessions-number*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a physical interface name. The value is like ge-1/1/1, te-1/1/3, etc.
max-sessions <*max-sessions-number*>	Specifies the maximum number of NAC sessions. The value is an integer in the range of 0 to 512. The default value is 0, indicating that there is no limit on the number of NAC sessions.

Usage Guidelines

This command is configured on a specified interface. Users can also configure the maximum number of NAC sessions globally by using the command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*>.

The maximum number of NAC sessions configured on an interface has a higher priority over the value configured globally.

Example

- Configure the maximum number of NAC sessions that are allowed to be established on interface ge-1/1/1 to 30.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 max-sessions 30
admin@Xorplus# commit
```

set protocols dot1x max-sessions-per-port

The **set protocols dot1x max-sessions-per-port** command globally configures the maximum number of NAC sessions that are allowed to be established on each port enabled for NAC.

Command Syntax

set protocols dot1x max-sessions-per-port <*max-sessions-number*>

Parameter

Parameter	Description
max-sessions-per-port <*max-sessions-number*>	Specifies the maximum number of NAC sessions. The value is an integer in the range of 0 to 512. The default value is 0, indicating that there is no limit on the number of NAC sessions.

Usage Guidelines

The command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*> is a global setting, which will take effect on all the interfaces enabled for NAC.

PicOS also provides the command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*> to configure the maximum number of NAC sessions that are allowed to be established on a specified interface.

The maximum number of NAC sessions configured on an interface has a higher priority over the value configured globally.

Example

- Configure the maximum number of NAC sessions that are allowed to be established on each interface enabled for NAC globally.

```
admin@Xorplus# set protocols dot1x max-sessions-per-port 30
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip auth-port

The **set protocols dot1x aaa radius authentication server-ip auth-port** command configures the UDP port of the RADIUS server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **auth-port** <*port-number*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
auth-port <*port-number*>	Specifies UDP port of RADIUS authentication server. The value is an integer that ranges from 1 to 65535. The default value is 1812.

Example

- Configure the UDP port of the RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 auth-port 5100
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip acct-port

The **set protocols dot1x aaa radius authentication server-ip acct-port** command configures the UDP port of the RADIUS accounting server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **acct-port** <*port-number*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
acct-port <*port-number*>	Specifies UDP port of RADIUS accounting server. The value is an integer that ranges from 1 to 65535. The default value is 1813.

Example

- Configure the UDP port of the RADIUS accounting server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 acct-port 5200
admin@Xorplus# commit
```

set protocols dot1x aaa radius dynamic-author client port

The **set protocols dot1x aaa radius dynamic-author client port** command configures the UDP port of the RADIUS dynamic authorization server for CoA function. This is the UDP port on the switch side.

Command Syntax

set protocols dot1x aaa radius dynamic-author client <*ip-address*> **port** <*port-number*>

Parameter

Parameter	Description
client <*ip-address*>	Specifies IPv4 address of the RADIUS dynamic authorization client. This is the IP address of the RADIUS server.
port <*port-number*>	Specifies UDP port of RADIUS dynamic authorization server. The value is an integer that ranges from 1 to 65535. The default value is 3799.

Example

- Configure the UDP port of the RADIUS dynamic authorization server.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 192.16.10.1 port 8888
admin@Xorplus# commit
```

run show dot1x radius-port

The **run show dot1x radius-port** command shows the UDP port information of 802.1X RADIUS server and dynamic authorization server for CoA.

Command Syntax

run show dot1x radius-port

Parameter

None.

Example

- View the UDP port information of 802.1X RADIUS server and dynamic authorization server for CoA.

```
admin@Xorplus# run show dot1x radius-port
Server-IP          Authentication     Accounting        CoA
---------------  ----------------    ----------------  ----------------
2.2.2.2            N/A                N/A               9999
5.5.5.5            N/A                N/A               3799
1.1.1.1            2222               1111              8888
3.3.3.3            6666               7777              N/A
4.4.4.4            1812               1813              N/A
```

NOTEs:

- “N/A” indicates related RADIUS service is not available. For example, in above show result, 2.2.2.2 and 5.5.5.5 are dynamic authorization clients for CoA only, and 4.4.4.4 is a RADIUS server for authentication and accounting without CoA.

  The UDP port number of 802.1X RADIUS server shows “N/A” if no RADIUS authentication server IP is configured. The UDP port number of dynamic authorization server of CoA shows “N/A” if no RADIUS dynamic authorization client IP is configured.

- The IP addresses of RADIUS dynamic authorization client are shown in the column “Server-IP”, as they are usually located on the RADIUS server.

set protocols dot1x filter sequence from destination-mac-address

NOTE:
This command is no longer supported from version 4.3.2, since this filter has been deprecated.

The **set protocols dot1x filter sequence from destination-mac-address** command configures the destination MAC address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter *<filter-name>* **sequence** *<sequence-number>* **from destination-mac-address** *<mac-address>*

Parameter

Parameter	Description
filter *<filter-name>*	Specifies the ACL filter name. The value is a string.
sequence *<sequence-number>*	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-mac-address *<mac-address>*	Specifies the destination MAC address of packets that match ACL rules. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Example

- Configure the destination MAC address of packets that match ACL rules to 10:50:ba:27:be:d2.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-mac-address 10:50:ba:27:be:d2
admin@Xorplus# commit
```

set protocols dot1x filter sequence from vlan

NOTE:
This command is no longer supported from version 4.3.2, since this filter has been deprecated.

The **set protocols dot1x filter sequence from vlan** command configures the VLAN ID information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from vlan** <*vlan-id*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Configure the VLAN ID of packets that match ACL rules to 100.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from vlan 100
admin@Xorplus# commit
```

SNMP Configuration Commands

- set protocols snmp trap-group targets security-name
- set protocols lldp snmp-trap
- set protocols snmp trap-group event cpu-threshold enable
- set protocols snmp trap-group event cpu-threshold high
- set protocols snmp trap-group event cpu-threshold interval
- set protocols snmp trap-group event cpu-threshold low
- set protocols snmp trap-group event mac-threshold enable
- set protocols snmp trap-group event mac-threshold interval
- set protocols snmp trap-group event mac-threshold limit
- set protocols snmp trap-group vrf mgmt-vrf
- set protocols snmp trap-group version
- set protocols snmp v3 enable
- set protocols snmp v3 usm-user
- set protocols snmp v3 usm-user group
- set protocols snmp v3 group notify-view
- set protocols snmp v3 group read-view
- set protocols snmp v3 group write-view
- set protocols snmp v3 group security-level
- set protocols snmp v3 usm-user authentication-mode
- set protocols snmp v3 usm-user authentication-key
- set protocols snmp v3 usm-user privacy-mode
- set protocols snmp v3 usm-user privacy-key
- set protocols snmp v3 mib-view subtree mask
- set protocols snmp v3 mib-view subtree type
- set protocols snmp trap-group source-interface
- set protocols snmp community
- set protocols snmp community authorization
- set protocols snmp community clients
- set protocols snmp contact
- set protocols snmp location
- run show snmp statistics

set protocols snmp trap-group targets security-name

The **set protocols snmp trap-group targets security-name** command configures NMS for receiving the trap messages.

> ⚠ Please note trap-messages can be actually sent out only if the concerning user, group and notify-view have been configured.

Command Syntax
set protocols snmp trap-group targets *<IPv4_address>* **security-name** <security-name>
delete protocols snmp trap-group targets *<IPv4_address>*

Parameter

Parameter	Description
targets *<IPv4_address>*	Specifies the address of the target host that receives SNMP traps. **NOTE:** The IP address specified by address and the security name specified by securityname together identify a target host.
security-name <security-name>	Specifies the user security name displayed on the NMS. For SNMPv3, **security name** must be configured as the user name. **security name** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **security name** configured. **security name** is used to distinguish multiple hosts that generate trap messages.

Example

•This example configures a NMS for receiving the trap messages.

```
admin@XorPlus# set protocols snmp trap-group targets 10.10.51.42 security-name user1
admin@XorPlus# commit
```

set protocols lldp snmp-trap

The **set protocols lldp snmp-trap** command is used to enable or disable the SNMP trap for LLDP function.

Command Syntax

set protocols lldp snmp-trap <**true** | **false**>

Parameter

Parameter	Description
snmp-trap <**true** | **false**>	Enable or disable the SNMP trap for LLDP function. The value could be **true** or **false**. • **true**: Enable the SNMP trap for LLDP function, the system can send LLDP trap message to NMS. • **false**: Disable the SNMP trap for LLDP function, then there will be no more LLDP trap message sends to NMS. The default value is **true**.

Example

- Disable the SNMP trap for LLDP function.

```
admin@Xorplus# set protocols lldp snmp-trap false
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold enable

The **set protocols snmp trap-group event cpu-threshold enable** command is used to enable or disable the function of monitoring the switch CPU usage and sending an SNMP Trap message when the switch CPU usage exceeds the overload threshold or falls below the low threshold.

Command Syntax

set protocols snmp trap-group event cpu-threshold enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the function of monitoring the switch CPU usage and sending an SNMP Trap message. The value could be **true** or **false**. • **true**: enables the function of monitoring the switch CPU usage and sending an SNMP Trap message. • **false**: disables the function of monitoring the switch CPU usage and sending an SNMP Trap message. The function is **disabled** by default.

Usage Guidelines

After this function is enabled, the device can generate an SNMP Trap alarm message when the switch CPU usage exceeds the overload threshold or falls below the low threshold, so you can effectively monitor CPU usage and optimize system performance to maintain data forwarding and network topology stability.

Example

- Enable the function of monitoring the switch CPU usage and sending an SNMP Trap message.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold enable true
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold high

The **set protocols snmp trap-group event cpu-threshold high** command sets the overload threshold for CPU usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event cpu-threshold high <*high-value*>

Parameter

Parameter	Description
high <*high-value*>	Specifies the overload threshold for CPU usage monitoring to send SNMP Trap messages. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 80.

Usage Guidelines

Use this command to set the CPU usage overload threshold. When CPU usage exceeds the overload threshold for a continuous time period, the system logs the event and sends an SNMP Trap message. By viewing log information, you can effectively monitor CPU usage.

NOTE:

- If the CPU usage reaches 100%, the system won't send SNMP Trap message.
- Please set the CPU usage monitoring overload threshold carefully. If the CPU usage overload threshold is set too small, the system generates alarms frequently. If the CPU usage overload threshold is set too large, you cannot be notified of the CPU usage overload in a timely manner.

Example

- Set the overload threshold for CPU usage to 80%.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold high 80
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold interval

The **set protocols snmp trap-group event cpu-threshold interval** command configures the time duration for which the CPU usage continues to exceed the overload threshold or fall below the low threshold.

Command Syntax

set protocols snmp trap-group event cpu-threshold interval *<interval>*

Parameter

Parameter	Description
interval *<interval>*	Specifies the time duration. The value is an integer, in seconds, that ranges from 5 to 4294967295. The default value is 300s.

Usage Guidelines

Generally, if the CPU usage of the system exceeds the threshold for a short period of time, the CPU usage is considered to be in the normal range, and no CPU usage alarm will be generated. Similarly, if the CPU usage falls below the low threshold but doesn't persist for the duration of **interval** time, again, no CPU usage alarm will be sent.

The system samples CPU usage one time every 5 seconds, if the CPU usage is out of the threshold range over this interval time, a SNMP trap message will be sent. But once CPU usage falls back into the threshold range and the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Example

- Configure the time duration when the CPU usage continues to exceed the overload threshold or fall below the low threshold to 300s.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold interval 300
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold low

The **set protocols snmp trap-group event cpu-threshold low** command configures sets the low threshold for CPU usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event cpu-threshold low <*low-value*>

Parameter

Parameter	Description
low <*low-value*>	Specifies the low threshold for CPU usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 20.

Usage Guidelines

When CPU usage falls below the low threshold for a continuous time period, the system logs the event and sends an SNMP Trap message. By viewing log information, you can effectively monitor CPU usage.

Example

- Set the low threshold for CPU usage to 20%.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold low 20
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold enable

The **set protocols snmp trap-group event mac-threshold enable** command is used to enable or disable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message when the switch MAC address table usage exceeds the limit threshold.

Command Syntax

set protocols snmp trap-group event mac-threshold enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. The value could be **true** or **false**. **true**: enables the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. **false**: disables the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. The function is **disabled** by default.

Usage Guidelines

After this function is enabled, the device can generate an SNMP Trap alarm message when the switch MAC address table usage exceeds the limit threshold, you can effectively monitor MAC address table usage and optimize system performance to maintain data forwarding and network topology stability.

Example

- Enable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold enable true
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold interval

The **set protocols snmp trap-group event mac-threshold interval** command configures the time duration when the MAC address table usage continues to exceed the limit threshold.

Command Syntax

set protocols snmp trap-group event mac-threshold interval *<interval>*

Parameter

Parameter	Description
interval *<interval>*	Specifies the time duration. The value is an integer, in minutes, that ranges from 5 to 4294967295. The default value is 15 minutes.

Usage Guidelines

The system samples MAC address table usage one time every 10 seconds, if the MAC address table usage exceed the limit threshold over this interval time, a SNMP trap message will be sent. But once MAC address table usage falls back below the threshold when the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Example

- Configure the time duration when the MAC address table usage continues to exceed the limit threshold to 50 minutes.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold interval 50
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold limit

The **set protocols snmp trap-group event mac-threshold limit** command sets the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event mac-threshold limit <*limit-value*>

Parameter

Parameter	Description
limit <*limit-value*>	Specifies the limit threshold for MAC address table usage monitoring to send SNMP Trap messages. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 50.

Usage Guidelines

Use this command to set the MAC address table usage limit threshold. When MAC address table usage exceeds the limit threshold over a continuous period of time, the system logs the event and sends an SNMP Trap message. By viewing log information, you can learn about MAC address table usage.

NOTE:

Please set the MAC address table usage monitoring limit threshold carefully. If the MAC address table usage limit threshold is set too small, the system generates alarms frequently. If the MAC address table usage limit threshold is set too large, you cannot get MAC address table usage overload immediately.

Example

- Set the limit threshold for MAC address table usage monitoring to 50%.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold limit 50
admin@Xorplus# commit
```

set protocols snmp trap-group vrf mgmt-vrf

The **set protocols snmp trap-group vrf mgmt-vrf** command configures to run the SNMP Trap service in the management VRF.

Command Syntax

set protocols snmp trap-group vrf mgmt-vrf

Parameter

None.

Usage Guidelines

SNMP Trap management service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding Network Management System (NMS) is required to be route reachable in the VRF running SNMP Trap management service.

Note: The latest configuration overrides the previous one.

Example

- Configure the SNMP Trap service to run in the management VRF.

```
admin@Xorplus# set protocols snmp trap-group vrf mgmt-vrf
admin@Xorplus# commit
```

set protocols snmp trap-group version

The **set protocols snmp trap-group version** command configures the version of the SNMP trap messages.The default version is v2.

Command Syntax
set protocols snmp trap-group version <*version*>
delete protocols snmp trap-group version <*version*>

Parameter

•<version> version of the trap messages

- **v1** version 1
- **v2** version 2
- **v3** version 3

Example

•This example configures version 3 to the trap messages

```
admin@XorPlus# set protocols snmp trap-group version v3
admin@XorPlus# commit
```

set protocols snmp v3 enable

The **set protocols snmp v3 enable** command can be used to enable or disable SNMPv3. The default version of the SNMP is v2.

Command Syntax
set protocols snmp v3 enable *<boolean>*

Parameter

Parameter	Description
enable *<boolean>*	Enable or disable SNMPv3. The value could be **true** or **false**. • **true**: enables SNMPv3. • **false**: disables SNMPv3. The default version of the SNMP is v2.

Example

•This example enables SNMPv3.

```
admin@XorPlus# set protocols snmp v3 enable true
admin@XorPlus# commit
```

set protocols snmp v3 usm-user

The **set protocols snmp v3 usm-user** command configures an SNMP user name.

> ⚠ A user without adding to any groups only can be read all the OIDs by NMS (could not be written or send trap-messages).

Command Syntax
set protocols snmp v3 usm-user <*user-name*>

delete protocols snmp v3 usm-user <*user-name*>

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.

Example

•This example configures a user user1 without adding to any groups.

```
admin@XorPlus# set protocols snmp v3 usm-user user1
admin@XorPlus# commit
```

set protocols snmp v3 usm-user group

> If you add a user to an SNMP group, you have to configure the read-view, write-view or notify-view for the group. Or NMS will have no authority (writing, reading, being notified) operated on the user.

The **set protocols snmp v3 usm-user group** command adds a user to an SNMP group.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **group** <*group-name*>

delete protocols snmp v3 usm-user <*user-name*> **group**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
group <*group-name*>	Specifies the name of the group to which a user belongs. The value is a string.

Example

•This example adds user1 to SNMP group1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 group group1
admin@XorPlus# commit
```

set protocols snmp v3 group notify-view

The **set protocols snmp v3 group notify-view** command configures a notify view for an SNMP group.

> ⚠ Some OIDs which are capable of sending trap-messages can be added to the notify-view optionally. If not doing so, the user will not send trap-messages initiatively.

Command Syntax
set protocols snmp v3 group <*group-name*> **notify-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **notify-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
notify-view <*view-name*>	Specifies a notify view. The value is a string.

Example

•This example configures a notify view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 notify-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group read-view

The **set protocols snmp v3 group read-view** command configures a read-only view for an SNMP group.

> A user in the group which is configured with read-view only can be read by NMS while cannot be written or send trap-messages. Writing and notifying authority can be gained by NMS only after you configure the corresponding view.

Command Syntax
set protocols snmp v3 group <*group-name*> **read-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **read-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
read-view <*view-name*>	Specifies a read-only view. The value is a string.

Example

•This example configures a read-view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 read-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group write-view

The **set protocols snmp v3 group write-view** command configures a read-write view for an SNMP group.

> A user in the group which is configured with write-view only can be written by NMS while cannot send trap-messages initiatively. Notify authority can be gained when you configure the corresponding view.

Command Syntax
set protocols snmp v3 group <*group-name*> **write-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **write-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
write-view <*view-name*>	Specifies a read-write view. The value is a string.

Example

•This example configures a write-view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 write-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group security-level

The **set protocols snmp v3 group security-level** command configure the security level of an SNMP group.

> When the security-level of a group is AuthNoPriv or AuthPriv,the user in that group should be configured with Authentication-mode, Authentication-key even as well as privacy-mode and privacy-key.

Command Syntax

set protocols snmp v3 group <*group-name*> **security-level** <**AuthNoPriv | AuthPriv | NoAuthNoPriv**>

delete protocols snmp v3 group <*group-name*> **security-level**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
security-level <**AuthNoPriv | AuthPriv | NoAuthNoPriv**>	Specifies the security level of the SNMP group. The value could be **AuthNoPriv**, **AuthPriv** or **NoAuthNoPriv.** • **AuthNoPriv**: authenticates SNMP messages without encryption. • **AuthPriv**: authenticates and encrypts SNMP messages. • **NoAuthNoPriv**: does not authenticate or encrypt SNMP messages.

Example

•This example configures group1 to AuthPriv.

```
admin@XorPlus# set protocols snmp v3 group group1 security-level AuthPriv
admin@XorPlus# commit
```

set protocols snmp v3 usm-user authentication-mode

The **set protocols snmp v3 usm-user authentication-mode** command configures authentication-mode for a user. If authentication-mode is configured, authentication-key also needs to be configured.

Command Syntax

set protocols snmp v3 usm-user <*user-name*> **authentication-mode** <**md5 | none | sha**>

delete protocols snmp v3 usm-user <*user-name*> **authentication-mode**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
authentication-mode <**md5	none	sha**>	Specifies the authentication-mode for a user. The value could be **md5**, **none** or **sha**. • **md5**: Specifies HMAC-MD5-96 as the authentication protocol. • **none**: Do not authenticate the user. • **sha**: Specifies HMAC-SHA-96 as the authentication protocol.

Example

•This example configures md5 authentication mode for user1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-mode md5
admin@XorPlus# commit
```

set protocols snmp v3 usm-user authentication-key

The **set protocols snmp v3 usm-user authentication-key** command configures a authentication key for a user.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **authentication-key** <*authentication-key*>

delete protocols snmp v3 usm-user <*user-name*> **authentication-key**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
authentication-key <*authentication-key*>	Specifies the authentication key for a user. The value is a string that should be no less than 8 characters.

Example

•This example configures a authentication-key for a user.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-key u1111key
admin@XorPlus# commit
```

set protocols snmp v3 usm-user privacy-mode

The **set protocols snmp v3 usm-user privacy-mode** command configures privacy-mode for a uese. If you have configured privacy-mode for a user, privacy-key also needs to be configured.

Command Syntax

set protocols snmp v3 usm-user <*user-name*> **privacy-mode** <*privacy-mode* >

delete protocols snmp v3 usm-user <*user-name*> **privacy-mode**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
privacy-mode <*privacy-mode* >	Specifies the encryption protocol for a user. The value could be **3des**, **aes128**, **des** or **none**.

Example

•This example configures **des** for user1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-mode des
admin@XorPlus# commit
```

set protocols snmp v3 usm-user privacy-key

The **set protocols snmp v3 usm-user privacy-key** command configures a privacy key for a user.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **privacy-key** <*privacy-key*>

delete protocols snmp v3 usm-user <*user-name*> **privacy-key**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
privacy-key <*privacy-key*>	Specifies the privacy key for a user. The value is a string that should be no less than 8 characters.

Example

•This example configures a privacy-key for a user.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-key u1111key
admin@XorPlus# commit
```

set protocols snmp v3 mib-view subtree mask

The **set protocols snmp v3 mib-view subtree mask** command configures a MIB view which is used as a view of a group. And users can just set up a mib-view without mask.

Command Syntax
set protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **mask** <*mask*>

delete protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **mask**

Parameter

Parameter	Description
mib-view <*view-name*>	Specifies the view name. The value is a string.
subtree <*oidtree*>	Specifies the OID for the MIB subtree. oid-tree can be the OID (such as 1.4.5.3.1) . **NOTE:** It must be a valid MIB subtree.
mask <*mask*>	Subtree mask in hexadecimal format with an even character.

Example

•This example configures a mib-view view1 with mask ff.

```
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 mask ff
admin@XorPlus# commit
```

set protocols snmp v3 mib-view subtree type

The **set protocols snmp v3 mib-view subtree type** command configures type of a MIB view.

Command Syntax
set protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **type** <**excluded | included**>

delete protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **type**

Parameter

•<text1> the name of the mib-view

•<text2> a dotted numeric oid

•<type> include or exclude a subtree

- **excluded** exclude the subtree
- **included** include the subtree

Parameter	Description
mib-view <*view-name*>	Specifies the view name. The value is a string.
subtree <*oidtree*>	Specifies the OID for the MIB subtree. oid-tree can be the OID (such as 1.4.5.3.1) . **NOTE:** It must be a valid MIB subtree.
type <**excluded | included**>	Specifies the MIB view type: • **excluded**: Excludes the MIB subtree. • **included**: Includes the MIB subtree.

Usage Guidelines

You can specify the MIB view based on the following rules:

- **excluded**: If a few MIB objects on the device or some objects in the current MIB view do not or no longer need to be managed by the NM station, **excluded** needs to be specified in the command to exclude these MIB objects.
- **included**: If a few MIB objects on the device or some objects in the current MIB view need to be managed by the NM station, **included** needs to be specified in the command to include these MIB objects.

Example

•This example includes 1.3.6.1.2.1 in the view1.

```
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 type included
admin@XorPlus# commit
```

set protocols snmp trap-group source-interface

The **set protocols snmp trap-group source-interface** command configures the source interface from which traps are sent.

Command Syntax

set protocols snmp trap-group source-interface <*source-interface*>

Parameter

Parameter	Description
source-interface <*source-interface*>	Specifies the source interface. The value could be **eth0**, loopback interface, routed interface, sub-interface or VLAN interface.

Usage Guidelines

You can run this command to specify the source interface on the device from which traps are sent. The specified source interface is used to derive the source IP address for the SNMP traps sent, so that traps received from each switch will always have a single consistent source IP address. To ensure device security, it is recommended that you set the source interface to the loopback interface.

Example

- Configure the loopback interface as the source interface from which traps are sent.

```
admin@Xorplus# set l3-interface loopback lo address 10.226.14.201 prefix-length 32
admin@Xorplus# set protocols snmp trap-group source-interface lo
admin@Xorplus# commit
```

set protocols snmp community

The **set protocols snmp community** command creates an SNMPv1 or SNMPv2c community name.

Command Syntax
set protocols snmp community <*community-name*>
delete protocols snmp community <*community-name*>

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.

Example

•This example configures a community name.

```
admin@XorPlus# set protocols snmp community comm1
admin@XorPlus# commit
```

set protocols snmp community authorization

The **set protocols snmp community authorization** command configures the authorization for an SNMP community.

Command Syntax
set protocols snmp community <*community-name*> **authorization** <**read-only | read-write**>
delete protocols snmp community <*community-name*> **authorization**

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.
authorization <**read-only	read-write**>	Specifies the authorization for an SNMP community. • **read-only**: Indicates that the community with a specified name has the read-only rights. • **read-write**: Indicates that the community with a specified name has the read-write rights.

Example

•This example configures the authorization for an SNMP community.

```
admin@XorPlus# set protocols snmp community comm1 authorization read-only
admin@XorPlus# commit
```

set protocols snmp community clients

The **set protocols snmp community clients** command configures the an SNMP client.

Command Syntax
set protocols snmp community <*community-name*> **clients** <*IP_address*>
delete protocols snmp community <*community-name*> **clients** <*IP_address*>

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.
clients <*IP_address*>	Specifies the IPv4 address of the SNMP client.

Example

•This example configures the an SNMP client.

```
admin@XorPlus# set protocols snmp community comm1 clients 10.10.10.1
admin@XorPlus# commit
```

set protocols snmp contact

The **set protocols snmp contact** command configures the contact information for system maintenance. If a device fails, maintenance engineer can contact the vendor for device maintenance.

Command Syntax
set protocols snmp contact <*contact*>
delete protocols snmp contact

Parameter

Parameter	Description
contact <*contact*>	Specifies contact information of system maintenance. The value is a string.

Example

•This example configures the contact information for system maintenance.

```
admin@XorPlus# set protocols snmp contact support.pica8.com
admin@XorPlus# commit
```

set protocols snmp location

The **set protocols snmp location** command configures the physical location information of the device.

Command Syntax
set protocols snmp location <*location*>
delete protocols snmp location

Parameter

Parameter	Description
location <*location*>	Specifies the physical location information of the device. The value is a string.

Example

•This example configures the physical location information of the device.

```
admin@XorPlus# set protocols snmp location CA:USA
admin@XorPlus# commit
```

run show snmp statistics

The **run show snmp statistics** command shows the SNMP messages statistics.

Command Syntax
run show snmp statistics

Parameter

None.

Example

•This example shows the SNMP messages statistics.

```
admin@XorPlus# run show snmp statistics
SNMP statistics:
Input:
Packets: 0, Bad versions: 0, Bad community names: 0,
Bad community uses: 0, ASN parse errors: 0,
Too bigs: 0, No such names: 0, Bad values: 0,
Read onlys: 0, General errors: 0,
Total request varbinds: 0, Total set varbinds: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0,
Silent drops: 0, Proxy drops 0
Output:
Packets: 0, Too bigs: 0, No such names: 0,
Bad values: 0, General errors: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0
```

Mirror Configuration Commands

- set interface ethernet-switching-options analyzer input
- set interface ethernet-switching-options analyzer output
- set interface ethernet-switching-options analyzer erspan input
- set interface ethernet-switching-options analyzer erspan output source-ip
- set interface ethernet-switching-options analyzer erspan output dest-ip
- set interface ethernet-switching-options analyzer erspan output vrf
- run show analyzer
- set firewall filter sequence then erspan source-ip
- set firewall filter sequence then erspan dest-ip
- set firewall filter sequence then erspan vrf
- set firewall filter sequence then erspan ttl

set interface ethernet-switching-options analyzer input

Port mirroring, is the duplication of traffic from a set of source ports onto a destination port. User can configure port mirroring to monitor and analyze source port traffic.

The **set interface ethernet-switching-options analyzer input** command configures source port, traffics of which need to be monitored. User can use the **set interface ethernet-switching-options analyzer output** command configure destination port.

Command Syntax

set interface ethernet-switching-options analyzer <*string*> **input** <**ingress | egress**> <*port*>

delete interface ethernet-switching-options analyzer <*string*> **input** <**ingress | egress**> <*port*>

Parameter

Parameter	Description
<*string*>	Specifies the name of a mirror, should consist of letters and/or numerals.
<**ingress	egress**>	Specifies the traffic direction of a source port.
<*port*>	Specifies ethernet switching port identifier of the source port.

NOTE：

- For Tomahawk platform switches, port mirroring can not be applied on both direction of the same source interface, that is, you can configure either ingress or egress traffic on the same source interface.
- One chassis switch supports a maximum of four input rules. For example, the following configurations are two input rules of analyzer 111 for the same source interface ge-1/1/3 of two different directions, ingress and egress.

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3

Example

• Configure ge-1/1/3 as the mirrored port, and ge-1/1/4 as the observing port.

```
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 output ge-1/1/4
admin@XorPlus# commit
```

set interface ethernet-switching-options analyzer output

Port mirroring, is the duplication of traffic from a set of source ports onto a destination port. User can configure port mirroring to monitor and analyze source port traffic.

The **set interface ethernet-switching-options analyzer output** command configures destination port, as the observing port of port mirroring. User can use the **set interface ethernet-switching-options analyzer input** command configure source port.

Command Syntax
set interface ethernet-switching-options analyzer <*string*> **output** <*port*>
delete interface ethernet-switching-options analyzer <*string*> **output** <*port*>

Parameter

Parameter	Description
<*string*>	Specifies the name of a mirror, should consist of letters and/or numerals.
<*port*>	Specifies ethernet switching port identifier of the destination port.

NOTE :

- For Tomahawk platform switches, port mirroring can not be applied on both direction of the same source interface, that is, you can configure either ingress or egress traffic on the same source interface.
- One chassis switch supports a maximum of four input rules. For example, the following configurations are two input rules of analyzer 111 for the same source interface ge-1/1/3 of two different directions, ingress and egress.

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3

Example
• Configure ge-1/1/3 as the mirrored port, and ge-1/1/4 as the observing port.

```
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 output ge-1/1/4
admin@XorPlus# commit
```

set interface ethernet-switching-options analyzer erspan input

The **set interface ethernet-switching-options analyzer erspan input** command configures the input port of ERSPAN. Parameter *ingress* indicates mirroring traffic in the inbound direction of the input port, *egress* indicates mirroring traffic in the outbound direction of the input port. You can configure to mirror both the ingress and egress traffic at the same time or only one direction.

The **delete interface ethernet-switching-options analyzer erspan input** command deletes the configuration.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input ingress**<*port-name*>

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input egress**<*port-name*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
<*port-name*>	Specifies the input port on which the traffic will be mirrored. Only physical interfaces are supported, any other interfaces, such as LAG interface, VLAN interfaces, are not supported.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output source-ip

The **set interface ethernet-switching-options analyzer erspan output source-ip** command configures the source IPv4 address for ERSPAN encapsulation.

The **delete interface ethernet-switching-options analyzer erspan output source-ip** command deletes the configuration.

> **NOTE:**
> The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output source-ip** <*source-ipv4*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
source-ip <*source-ipv4*>	Specifies the source IPv4 address for the IP header encapsulation in the outer layer of the GRE message.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output dest-ip

The **set interface ethernet-switching-options analyzer erspan output dest-ip** command configures the destination IP address for ERSPAN encapsulation.

The **delete interface ethernet-switching-options analyzer erspan output dest-ip** command deletes the configuration.

NOTEs:

- The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.
- The specified destination IP address should be configured the same as the IP address of the remote Data Monitoring Server to ensure the destination is reachable for the mirrored messages.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output dest-ip** <*dest-ipv4*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
dest-ip <*dest-ipv4*>	Specifies the destination IPv4 address for the IP header encapsulation in the outer layer of the GRE message.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output vrf

The **set interface ethernet-switching-options analyzer erspan output vrf** command configures the VRF of the ERSPAN GRE tunnel of destination interface. Note that you have to ensure the remote data monitoring server is route reachable in the VRF.

The **delete interface ethernet-switching-options analyzer erspan output vrf** command deletes the configuration.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output vrf** <*vrf-name*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
vrf <*vrf-name*>	Specifies the VRF name of the GRE tunnel for ERSPAN.

Example

- Configure VRF of the GRE tunnel for ERSPAN.

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output vrf vrf1
admin@Xorplus# commit
```

run show analyzer

The **run show analyzer** command is used to view the mirroring information.

Command Syntax

run show analyzer [<*mirror-name*>]

Parameter

Parameter	Description
<*mirror-name*>	Optional. Specifies a name of the ERSPN. The value is a string.

Example

- View mirror configuration information.

```
admin@PICOS# run show analyzer
Analyzer name: 111
Erspan Output:
       state: UP
       source-ip: 10.10.10.1
       dest-ip: 20.20.20.1
       output-port: ge-1/1/3
       tagged vlan:
       vrf:
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces:

Analyzer name: 3
Output interface: <ge-1/1/5>
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces:

admin@SwitchB# run show analyzer 111
Analyzer name: 111
Output interface: <ge-1/1/2>
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces: <ge-1/1/1>
```

set firewall filter sequence then erspan source-ip

The **set firewall filter sequence then erspan source-ip** command configures the source IP address for ACL-based ERSPAN encapsulation for the packets matching the ACL rule.

If ACL-based ERSPAN is configured, PICOS copies service flows matching the rules to the output port, and then forwards the mirrored messages to the remote monitoring device through the GRE tunnel for analysis and monitoring. This command configures the source IP address of the GRE tunnel.

The **delete firewall filter sequence then erspan source-ip** command deletes the configuration.

> **NOTE:**
> The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan source-ip** <*source-ip*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
source-ip <*source-ip*>	Specifies the source IP address of the GRE tunnel of ERSPAN destination interface.

Example

- The following example commands mirror the packets matching the ACL rule that te-1/1/1 receives, and copy and transmit the packets from source IP address 4.4.4.4 to destination IP address 8.8.8.8through a GRE tunnel:

```
admin@Xorplus# set firewall filter f1 sequence 1 from protocol tcp
admin@Xorplus# set firewall filter f1 sequence 1 from source-address-ipv4 1.1.1.1/32
admin@Xorplus# set firewall filter f1 input interface te-1/1/1
admin@Xorplus# set firewall filter f1 sequence 1 then erspan source-ip 4.4.4.4
admin@Xorplus# set firewall filter f1 sequence 1 then erspan dest-ip 8.8.8.8
admin@Xorplus# commit
```

set firewall filter sequence then erspan dest-ip

The **set firewall filter sequence then erspan dest-ip** command configures the destination IP address for ACL-based ERSPAN encapsulation for the packets matching the ACL rule.

If ACL-based ERSPAN is configured, PICOS copies service flows matching the rules to the output port, and then forwards the mirrored messages to the remote monitoring device through the GRE tunnel for analysis and monitoring. This command configures the destination IP address of the GRE tunnel.

The **delete interface ethernet-switching-options analyzer erspan output dest-ip** command deletes the configuration.

NOTEs:

- The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.
- The specified destination IP address should be configured the same as the IP address of the remote Data Monitoring Server to ensure the destination is reachable for the mirrored messages.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan dest-ip** <*dest-ip*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
dest-ip <*dest-ip*>	Specifies the destination IP address of the GRE tunnel of ERSPAN destination interface.

Example

- The following example commands mirror the packets matching the ACL rule that te-1/1/1 receives, and copy and transmit the packets from source IP address 4.4.4.4 to destination IP address 8.8.8.8 through a GRE tunnel:

```
admin@Xorplus# set firewall filter f1 sequence 1 from protocol tcp
admin@Xorplus# set firewall filter f1 sequence 1 from source-address-ipv4 1.1.1.1/32
admin@Xorplus# set firewall filter f1 input interface te-1/1/1
admin@Xorplus# set firewall filter f1 sequence 1 then erspan source-ip 4.4.4.4
admin@Xorplus# set firewall filter f1 sequence 1 then erspan dest-ip 8.8.8.8
admin@Xorplus# commit
```

set firewall filter sequence then erspan vrf

The **set firewall filter sequence then erspan vrf** command configures the VRF of the ACL-based ERSPAN GRE tunnel. Note that you have to ensure the remote data monitoring server is route reachable in the VRF.

The **delete firewall filter sequence then erspan vrf** command deletes the configuration.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan vrf** <*vrf-name*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
vrf <*vrf-name*>	Specifies the VRF of the ACL-based ERSPAN GRE tunnel. The value is a string.

Example

- Configure VRF of the GRE tunnel for ACL-based ERSPAN.

```
admin@Xorplus# set firewall filter f1 sequence 1 then erspan vrf vrf1
admin@Xorplus# commit
```

set firewall filter sequence then erspan ttl

The **set firewall filter sequence then erspan ttl** command configures the Time-To-Life (TTL) value of the ACL-based ERSPAN packets.

The **delete firewall filter sequence then erspan ttl** command deletes the configuration.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan ttl** <*ttl-value*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
ttl <*ttl-value*>	Specifies the TTL value of the ACL-based ERSPAN packets. The value is an integer that ranges from 1 to 255. The default value is 255.

Example

- Configure TTL value of the ACL-based ERSPAN packets to 64.

```
admin@Xorplus# set firewall filter f1 sequence 1 then erspan ttl 64
admin@Xorplus# commit
```

RMON Commands

- run show rmon alarms
- run show rmon eventlog
- run show rmon events
- run show rmon history
- run show rmon statistics
- set protocols snmp rmon alarm falling-event-index
- set protocols snmp rmon alarm falling-threshold
- set protocols snmp rmon alarm interval
- set protocols snmp rmon alarm owner
- set protocols snmp rmon alarm rising-event-index
- set protocols snmp rmon alarm rising-threshold
- set protocols snmp rmon alarm sample-type
- set protocols snmp rmon alarm variable
- set protocols snmp rmon event community
- set protocols snmp rmon event description
- set protocols snmp rmon event owner
- set protocols snmp rmon event type
- set protocols snmp rmon history buckets
- set protocols snmp rmon history interface
- set protocols snmp rmon history interval
- set protocols snmp rmon history owner
- set protocols snmp rmon statistics interface
- set protocols snmp rmon statistics owner

run show rmon alarms

The **run show rmon alarms** command is used to view RMON alarms information.

Command Syntax

run show rmon alarms [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON alarms table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON alarms information.

```
admin@PICOS# run show rmon alarms
Entry 1 is active, and owned by monitor
    Monitors 1.3.6.1.2.1.16.1.1.1.4.1 every 10 seconds
    Taking absolute samples, last value was 369804
    Rising threshold is 1000000000, assigned to event 1
    Falling threshold is 1000000000, assigned to event 1
    On startup enable rising or falling alarm
```

run show rmon eventlog

The **run show rmon eventlog** command is used to view RMON event log information.

Command Syntax

run show rmon eventlog [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON event log table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON event log information.

```
admin@PICOS# run show rmon eventlog
Entry 1 owned by monitor is VALID.
    Generates eventLog 1.1 at 0:01:19.
    Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarmEntry 1, equal or lesser than 1000000000 with alarm v
```

run show rmon events

The **run show rmon events** command is used to view RMON event information.

Command Syntax

run show rmon events [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON event information.

```
admin@PICOS# run show rmon events
Entry 1 is active, and owned by monitor,
    Description is test,
    Event firing causes trap to community public,
    Last event fired at 0:01:19,
    Current uptime 1:02:17.
```

run show rmon history

The **run show rmon history** command is used to view RMON history statistics information.

Command Syntax

run show rmon history [*<entry-index>*]

Parameter

Parameter	Description
[*<entry-index>*]	Optional. Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON history statistics information.

```
admin@PICOS# run show rmon history
Entry 3 on ge-1/1/21 is active, and owned by monitor,
    Monitors ifIndex.21 every 10 seconds, bucket is 50,
        Sample # 1 began measuring at 0:43:22
            Received 576000 octets, 9000 packets,
            0 broadcast and 9000 multicast packets,
            0 undersized and 0 oversized packets,
            0 fragments and 0 jabbers,
            0 CRC alignment errors and 0 collisions.
            network utilization is estimated at 0
```

run show rmon statistics

The **run show rmon statistics** command is used to view RMON Ethernet statistics information.

Command Syntax

run show rmon statistics [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON statistics table index. The value is an integer that ranges from 1 to 255.

Example

- View RMON Ethernet statistics information.

```
admin@PICOS# run show rmon statistics
Entry 1 on ge-1/1/4 is active, and owned by monitor,
    Monitors ifIndex.4 which has
    Received 354601 octets, 3643 packets,
    0 broadcast and 0 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    dropped packet events (due to lack of resources):0.
    packets received of length (in octets):
        64: 0, 65-127: 3524, 128-255: 119,
        256-511: 0, 512-1023: 0, 1024-1518: 0
```

set protocols snmp rmon alarm falling-event-index

The **set protocols snmp rmon alarm falling-event-index** command configures the event to fire when the alarm falling threshold is crossed.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm *<entry-index>* **falling-event-index** *<alarmFallingEventIndex>*

delete protocols snmp rmon alarm *<entry-index>*

Parameters

Parameter	Description
alarm *<entry-index>*	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
falling-event-index *<alarmFallingEventIndex>*	Specifies the event to fire when the alarm falling threshold is crossed. The value is an integer that is configured in command **set protocols snmp rmon event** *<entry-index> XX*. When configured to 0, it indicates no event has been specified, so no action will be taken when the alarm threshold is exceeded.

Example

- Configure the event to fire when the falling threshold is crossed.

```
admin@PICOS# set protocols snmp rmon alarm 1 falling-event-index 5
admin@PICOS# commit
```

set protocols snmp rmon alarm falling-threshold

The **set protocols snmp rmon alarm falling-threshold** command configures the falling threshold of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm *<entry-index>* **falling-threshold** *<alarmFallingThreshold>*

delete protocols snmp rmon alarm *<entry-index>*

Parameters

Parameter	Description
alarm *<entry-index>*	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
falling-threshold *<alarmFallingThreshold>*	Specifies the falling threshold. The value is an integer that ranges from 0 to 2147483647.

Usage Guidelines

Rising threshold and falling threshold are a pair of values for a monitoring object, both values need to be configured for the same alarm entry.

In the following configuration example, the alarm event is triggered when the rising threshold 600 is exceeded, and the alarm event is triggered again when the monitoring value falls back to the falling threshold 400.

```
admin@Switch# set protocols snmp rmon alarm 1 rising-threshold 600
admin@Switch# set protocols snmp rmon alarm 1 rising-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 falling-threshold 400
admin@Switch# set protocols snmp rmon alarm 1 falling-event-index 1
```

Example

- Configure the falling threshold of the RMON alarm to 600.

```
admin@PICOS# set protocols snmp rmon alarm 1 falling-threshold 600
admin@PICOS# commit
```

set protocols snmp rmon alarm interval

The **set protocols snmp rmon alarm interval** command configures the sampling interval of RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **interval** <*interval*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
interval <*interval*>	Specifies the sampling interval for RMON alarm. The value is an integer, in seconds, that ranges from 10 to 3600.

Example

- Configure the sampling interval of RMON alarm to 20 seconds.

```
admin@PICOS# set protocols snmp rmon alarm 1 interval 20
admin@PICOS# commit
```

set protocols snmp rmon alarm owner

The **set protocols snmp rmon alarm owner** command configures the owner's name of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **owner** <*owner*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
owner <*owner*>	Specifies the owner's name of the RMON alarm. The value is a string.

Example

- Configure the owner for the RMON alarm.

```
admin@PICOS# set protocols snmp rmon alarm 1 owner public
admin@PICOS# commit
```

set protocols snmp rmon alarm rising-event-index

The **set protocols snmp rmon alarm rising-event-index** command configures the event to fire when the alarm rising threshold is crossed.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **rising-event-index** <*alarmRisingEventIndex*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 0 to 65535.
rising-event-index <*alarmRisingEventIndex*>	Specifies the event to fire when the alarm rising threshold is crossed. The value is an integer that is configured in command **set protocols snmp rmon event** <*entry-index*> *XX*. When configured to 0, it indicates no event has been specified, so no action will be taken when the alarm threshold is exceeded.

Example

- Configure the event to fire when the rising threshold is crossed.

```
admin@PICOS# set protocols snmp rmon alarm 1 rising-event-index 5
admin@PICOS# commit
```

set protocols snmp rmon alarm rising-threshold

The **set protocols snmp rmon alarm rising-threshold** command configures the rising threshold of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **rising-threshold** <*alarmRisingThreshold*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
rising-threshold <*alarmRisingThreshold*>	Specifies the rising threshold. The value is an integer that ranges from 0 to 2147483647.

Usage Guidelines

Rising threshold and falling threshold are a pair of values for a monitoring object, both values need to be configured for the same alarm entry.

In the following configuration example, the alarm event is triggered when the rising threshold 600 is exceeded, and the alarm event is triggered again when the monitoring value falls back to the falling threshold 400.

```
admin@Switch# set protocols snmp rmon alarm 1 rising-threshold 600
admin@Switch# set protocols snmp rmon alarm 1 rising-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 falling-threshold 400
admin@Switch# set protocols snmp rmon alarm 1 falling-event-index 1
```

Example

- Configure the rising threshold of the RMON alarm to 600.

```
admin@PICOS# set protocols snmp rmon alarm 1 rising-threshold 600
admin@PICOS# commit
```

set protocols snmp rmon alarm sample-type

The **set protocols snmp rmon alarm sample-type** command configures the sampling type of RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **sample-type** <**absolute** | **delta**>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
sample-type <**absolute**	**delta**>	Specifies the sampling type for RMON alarm. The value could be **absolute** or **delta**. • **absolute**: If the sample type is absolute, this value will be the sampled value at the end of the period. • **delta**: If the sample type is delta, this value will be the difference between the samples at the beginning and end of the period.

Example

- Configure the sampling type of RMON alarm to **delta**.

```
admin@PICOS# set protocols snmp rmon alarm 1 sample-type delta
admin@PICOS# commit
```

set protocols snmp rmon alarm variable

The **set protocols snmp rmon alarm variable** command configures SNMP MIB OID of the RMON alarm monitoring object.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm *<entry-index>* **variable** *<oid-variable>*

delete protocols snmp rmon alarm *<entry-index>*

Parameters

Parameter	Description
alarm *<entry-index>*	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
variable *<oid-variable>*	Specifies SNMP MIB OID of the RMON alarm. The value is a string.

Example

- Configure a RMON alarm for OID of 1.3.6.1.2.1.16.1.1.1.4.1.

```
admin@PICOS# set protocols snmp rmon alarm 1 variable 1.3.6.1.2.1.16.1.1.1.4.1
admin@PICOS# commit
```

set protocols snmp rmon event community

The **set protocols snmp rmon event community** command configures the community for the RMON event.

Note:

The **community** setting here should be consistent with the value of **community** and **security-name** in SNMP trap configuration.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **community** <*community*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
community <*community*>	Specifies the name of a community. The value is a string. The default value is **public**.

Example

- Configure the community for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 community comm1
admin@PICOS# commit
```

set protocols snmp rmon event description

The **set protocols snmp rmon event description** command configures the description for the RMON event.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **description** <*event_description*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
description <*event_description*>	Specifies the description for the RMON event. The value is a string.

Example

- Configure the description for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 description AlarmEvent
admin@PICOS# commit
```

set protocols snmp rmon event owner

The **set protocols snmp rmon event owner** command configures the owner's name of the RMON event.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **owner** <*owner*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
owner <*owner*>	Specifies the owner's name of the RMON event. The value is a string.

Example

- Configure the owner for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 owner public
admin@PICOS# commit
```

set protocols snmp rmon event type

The **set protocols snmp rmon event type** command configures the RMON event action type.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **type** <**none** | **log** | **trap** | **log-trap**>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
type <**none** | **log** | **trap** | **log-trap**>	Specifies RMON event action type. The value could be **none**, **log**, **trap** or **log-trap**. • **none**: Nothing will be done if the event is triggered. • **log**: If the event is triggered, an entry will be made in the logTable. • **trap**: If the event is triggered, an SNMP trap will be sent to the management station. • **log-trap**: If the event is triggered, both the log and trap action will be taken.

Usage Guidelines

When type is **trap** or **log-trap**, you need to configure SNMP trap function.

Example

- Configure the RMON event action type to **log**.

```
admin@PICOS# set protocols snmp rmon event 1 type log
admin@PICOS# commit
```

set protocols snmp rmon history buckets

The **set protocols snmp rmon history buckets** command configures the history statistics table capacity, that is, the maximum number of records that the history table can hold.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **buckets** <*number*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
buckets <*number*>	Specifies the history statistics table capacity, that is, the maximum number of records that the history table can hold. The value is an integer that ranges from 1 to 65535.

Example

- Configure the history statistics table capacity to 100.

```
admin@PICOS# set protocols snmp rmon history 1 buckets 100
admin@PICOS# commit
```

set protocols snmp rmon history interface

The **set protocols snmp rmon history interface** command configures RMON history statistics on a specified interface.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **interface** <*interface-name*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
interface <*interface-name*>	Specifies the interface for RMON history statistics. The value could be a physical interface or LAG interface.

Usage Guidelines

RMON historical statistics collects statistics periodically, but only the latest statistics are stored. The maximum number of records that the history table can hold is configured by command **set protocols snmp rmon history** *<entry-index>* **buckets** <*number*>.

Example

- Configure RMON history statistics on interface ge-1/1/1.

```
admin@PICOS# set protocols snmp rmon history 1 interface ge-1/1/1
admin@PICOS# commit
```

set protocols snmp rmon history interval

The **set protocols snmp rmon history interval** command configures the sampling interval of RMON history statistics.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **interval** <*interval*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
interval <*interval*>	Specifies the sampling interval for RMON history statistics. The value is an integer, in seconds, that ranges from 10 to 3600.

Example

- Configure the sampling interval of RMON history statistics to 20 seconds.

```
admin@PICOS# set protocols snmp rmon history 1 interval 20
admin@PICOS# commit
```

set protocols snmp rmon history owner

The **set protocols snmp rmon history owner** command configures the owner's name of the RMON history statistics table.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **owner** <*string*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
owner <*string*>	Specifies the owner's name of the RMON statistics table. The value is a string.

Example

- Configure the owner's name of the RMON history statistics table.

```
admin@PICOS# set protocols snmp rmon history 1 owner owner_pica8
admin@PICOS# commit
```

set protocols snmp rmon statistics interface

The **set protocols snmp rmon statistics interface** command configures RMON ethernet statistics on a specified interface. After the statistics table entry is configured under the specified interface, the system continuously gathers statistics for the number of messages on the interface.

The **delete protocols snmp rmon statistics** command deletes the configuration. Users need to delete the RMON ethernet statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon statistics <*entry-index*> **interface** <*interface-name*>

delete protocols snmp rmon statistics <*entry-index*>

Parameters

Parameter	Description
statistics <*entry-index*>	Specifies the RMON ethernet statistics table index. The value is an integer that ranges from 1 to 255.
interface <*interface-name*>	Specifies the interface for RMON ethernet statistics. The value could be a physical interface or LAG interface.

Example

- Configure RMON ethernet statistics on interface ge-1/1/1.

```
admin@PICOS# set protocols snmp rmon statistics 1 interface ge-1/1/1
admin@PICOS# commit
```

set protocols snmp rmon statistics owner

The **set protocols snmp rmon statistics owner** command configures the owner's name of the RMON ethernet statistics table.

The **delete protocols snmp rmon statistics** command deletes the configuration. Users need to delete the RMON ethernet statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon statistics *<entry-index>* **owner** *<string>*

delete protocols snmp rmon statistics *<entry-index>*

Parameters

Parameter	Description
statistics *<entry-index>*	Specifies the RMON ethernet statistics table index. The value is an integer that ranges from 1 to 255.
owner *<string>*	Specifies the owner's name of the RMON ethernet statistics table. The value is a string.

Example

- Configure the owner's name of the RMON ethernet statistics table.

```
admin@PICOS# set protocols snmp rmon statistics 1 owner owner_pica8
admin@PICOS# commit
```

RESTCONF Commands

- set protocols restconf
- set protocols restconf port
- set protocols restconf traceoptions flag config disable
- set protocols restconf traceoptions flag all disable
- set protocols restconf traceoptions flag datastore disable

set protocols restconf

The **set protocols restconf** command enables RESTCONF function on RESTCONF server. By default, RESTCONF is disabled.

The **delete protocols restconf** command disables RESTCONF on RESTCONF server.

Command Syntax

set protocols restconf

delete protocols restconf

Parameters

None.

Example

- Enable RESTCONF on RESTCONF server.

```
admin@PICOS# set protocols restconf
admin@PICOS# commit
```

set protocols restconf port

The **set protocols restconf port** command configures RESTCONF service listening port on RESTCONF server. By default, the RESTCONF service port number is 443.

The **delete protocols restconf port** command restores the configuration to the default value on RESTCONF server.

> **NOTE**:
>
> The RESTCONF service listening port in the HTTP request URL sent by RESTCONF Client needs to be consistent with the port configured on the server side.

Command Syntax

set protocols restconf port <*port-number*>

delete protocols restconf port

Parameter

Parameter	Description
port <*port-number*>	Specifies RESTCONF service listening port. The value is an integer that ranges from 1024 to 65535. The default value is 443.

Example

- Configure RESTCONF service listening port to 1024 on RESTCONF server.

```
admin@PICOS# set protocols restconf port 1024
admin@PICOS# commit
```

set protocols restconf traceoptions flag config disable

The **set protocols restconf traceoptions flag config disable** command can be used to enable or disable RESTCONF debugging for configuration tracing.

The **delete protocols restconf traceoptions flag config disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag config disable <**true | false**>

delete protocols restconf traceoptions flag config disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable RESTCONF debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable RESTCONF debugging for configuration tracing. • **false**: Enable RESTCONF debugging for configuration tracing. By default, RESTCONF debugging for configuration tracing is disabled.

Example

- Enable RESTCONF debugging for configuration tracing.

```
admin@PICOS# set protocols restconf traceoptions flag config disable false
admin@PICOS# commit
```

set protocols restconf traceoptions flag all disable

The **set protocols restconf traceoptions flag all disable** command can be used to enable or disable RESTCONF debugging for tracing all RESTCONF operations.

The **delete protocols restconf traceoptions flag all disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag all disable <**true | false**>

delete protocols restconf traceoptions flagall disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable RESTCONF debugging for tracing all RESTCONF operations. The value could be **true** or **false**. • **true**: Disable RESTCONF debugging for tracing all RESTCONF operations. • **false**: Enable RESTCONF debugging for tracing all RESTCONF operations. By default, RESTCONF debugging for tracing all RESTCONF operations is disabled.

Example

- Enable RESTCONF debugging for tracing all RESTCONF operations.

```
admin@PICOS# set protocols restconf traceoptions flag all disable false
admin@PICOS# commit
```

set protocols restconf traceoptions flag datastore disable

The **set protocols restconf traceoptions flag datastore disable** command can be used to enable or disable debugging about the RESTCONF datastore operation.

The **delete protocols restconf traceoptions flag datastore disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag datastore disable <**true | false**>

delete protocols restconf traceoptions flag datastore disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable debugging about the RESTCONF datastore operation. The value could be **true** or **false**. • **true**: Disable debugging about the RESTCONF datastore operation. • **false**: Enable debugging about the RESTCONF datastore operation. By default, debugging about the RESTCONF datastore operation is disabled.

Example

- Enable debugging about the RESTCONF datastore operation.

```
admin@PICOS# set protocols restconf traceoptions flag datastore disable false
admin@PICOS# commit
```

run show system boot-messages

The **run show system boot-message** command displays information about boot time messages. The command displays copyright, up time, revision, using MPC85 xx CDS machine description, etc.

Command Syntax
run show system boot-messages

Example
• This example demonstrates how to show system boot-messages:

```
admin@XorPlus# run show system boot-messages
Copyright (c) 2009-2014 Pica8 Inc.
All rights reserved.
Up time: 13:03:50
revision: 2.6.27
Using MPC85xx CDS machine description
Memory CAM mapping: CAM0=256Mb, CAM1=256Mb, CAM2=0Mb residual: 0Mb
Linux version 2.6.27 (root@dev-18) (gcc version 4.2.2) #49 Fri Apr 25 11:19:13 CST 2014
Found legacy serial port 0 for /soc8541@e0000000/serial@4500
  mem=e0004500, taddr=e0004500, irq=0, clk=330000000, speed=0
console [udbg0] enabled
Found FSL PCI host bridge at 0x00000000e0008000. Firmware bus number: 0->0
PCI host bridge /pci@e0008000 (primary) ranges:
 MEM 0x0000000080000000..0x000000009fffffff -> 0x0000000080000000
  IO 0x00000000e2000000..0x00000000e20fffff -> 0x0000000000000000
Top of RAM: 0x20000000, Total RAM: 0x20000000
Memory hole size: 0MB
Zone PFN ranges:
  DMA      0x00000000 -> 0x00020000
  Normal   0x00020000 -> 0x00020000
  HighMem  0x00020000 -> 0x00020000
Movable zone start PFN for each node
early_node_map[1] active PFN ranges
    0: 0x00000000 -> 0x00020000
On node 0 totalpages: 131072
free_area_init_node: node 0, pgdat c03cc4d4, node_mem_map c0404000
  DMA zone: 130048 pages, LIFO batch:31
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 130048
Kernel command line: root=/dev/hda1 rw noinitrd console=ttyS0,115200
mpic: Setting up MPIC " OpenPIC  " version 1.2 at e0040000, max 1 CPUs
mpic: ISU size: 56, shift: 6, mask: 3f
mpic: Initializing for 56 sources
PID hash table entries: 2048 (order: 11, 8192 bytes)
time_init: decrementer frequency = 41.250000 MHz
time_init: processor frequency   = 825.000000 MHz
clocksource: timebase mult[60f83e1] shift[22] registered
clockevent: decrementer mult[a8f] shift[16] cpu[0]
Console: colour dummy device 80x25
Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
High memory: 0k
Memory: 515456k/524288k available (3764k kernel code, 8648k reserved, 132k data, 162k bss, 168k init)
SLUB: Genslabs=12, HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Calibrating delay loop... 82.43 BogoMIPS (lpj=164864)
 --More--
```

run show system connections

The **run show system connections** command displays information about the system connection activity. It includes servers and established. The command displays Proto, .Recv-q, Send-Q, Local Address, Foreign Address, State, User, and Inode.

Command Syntax
run show system connections

Example
• This example demonstrates how to show system connections:

```
admin@XorPlus# run show system connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode
tcp        0      0 127.0.0.1:44992         0.0.0.0:*               LISTEN      11         34882
tcp        0      0 127.0.0.1:41248         0.0.0.0:*               LISTEN      0          1458
tcp        0      0 127.0.0.1:56961         0.0.0.0:*               LISTEN      11         7095
tcp        0      0 127.0.0.1:42946         0.0.0.0:*               LISTEN      0          2614
tcp        0      0 127.0.0.1:43938         0.0.0.0:*               LISTEN      0          1406
tcp        0      0 127.0.0.1:50436         0.0.0.0:*               LISTEN      0          2653
tcp        0      0 127.0.0.1:51622         0.0.0.0:*               LISTEN      0          2620
tcp        0      0 127.0.0.1:54214         0.0.0.0:*               LISTEN      0          2618
tcp        0      0 127.0.0.1:47143         0.0.0.0:*               LISTEN      0          4411
tcp        0      0 127.0.0.1:36455         0.0.0.0:*               LISTEN      0          1462
tcp        0      0 127.0.0.1:39592         0.0.0.0:*               LISTEN      0          1466
tcp        0      0 127.0.0.1:53512         0.0.0.0:*               LISTEN      0          1319
tcp        0      0 127.0.0.1:57354         0.0.0.0:*               LISTEN      0          4257
tcp        0      0 127.0.0.1:33197         0.0.0.0:*               LISTEN      0          4400
tcp        0      0 127.0.0.1:58765         0.0.0.0:*               LISTEN      0          1460
tcp        0      0 127.0.0.1:55985         0.0.0.0:*               LISTEN      0          1456
tcp        0      0 127.0.0.1:56564         0.0.0.0:*               LISTEN      0          2577
tcp        0      0 127.0.0.1:44756         0.0.0.0:*               LISTEN      0          1464
tcp        0      0 127.0.0.1:51957         0.0.0.0:*               LISTEN      0          1468
tcp        0      0 127.0.0.1:44086         0.0.0.0:*               LISTEN      11         66976
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          3364
tcp        0      0 127.0.0.1:51222         0.0.0.0:*               LISTEN      0          2575
tcp        0      0 127.0.0.1:53208         0.0.0.0:*               LISTEN      0          4252
tcp        0      0 127.0.0.1:56441         0.0.0.0:*               LISTEN      0          2616
tcp        0      0 127.0.0.1:37210         0.0.0.0:*               LISTEN      0          4286
tcp        0      0 127.0.0.1:29595         0.0.0.0:*               LISTEN      0          1316
tcp        0      0 127.0.0.1:38492         0.0.0.0:*               LISTEN      0          1454
tcp        0      0 127.0.0.1:52988         0.0.0.0:*               LISTEN      0          1452
tcp        0      0 127.0.0.1:50206         0.0.0.0:*               LISTEN      0          1450
tcp        0      0 127.0.0.1:29595         127.0.0.1:45862         ESTABLISHED 0          2637
tcp        0      0 127.0.0.1:55985         127.0.0.1:34260         ESTABLISHED 0          4295
tcp        0      0 127.0.0.1:57004         127.0.0.1:50206         ESTABLISHED 0          1629
tcp        0      0 127.0.0.1:38841         127.0.0.1:57354         ESTABLISHED 0          4264
tcp        0      0 127.0.0.1:41248         127.0.0.1:33787         ESTABLISHED 0          4271
tcp        0      0 127.0.0.1:29595         127.0.0.1:45845         ESTABLISHED 0          1485
tcp        0      0 127.0.0.1:59503         127.0.0.1:50436         ESTABLISHED 0          2696
tcp        0      0 127.0.0.1:29595         127.0.0.1:45854         ESTABLISHED 0          2579
tcp        0      0 127.0.0.1:54304         127.0.0.1:44086         ESTABLISHED 0          67026
tcp        0      0 127.0.0.1:57039         127.0.0.1:50206         ESTABLISHED 0          4266
tcp        0      0 127.0.0.1:44118         127.0.0.1:43938         ESTABLISHED 0          2222
tcp        0      0 127.0.0.1:43938         127.0.0.1:44162         ESTABLISHED 0          4418
tcp        0      0 127.0.0.1:29595         127.0.0.1:45879         ESTABLISHED 0          4254
tcp        0      0 127.0.0.1:41078         127.0.0.1:37210         ESTABLISHED 0          4292
tcp        0      0 127.0.0.1:41077         127.0.0.1:37210         ESTABLISHED 0          4289
tcp        0      0 127.0.0.1:55264         127.0.0.1:33197         ESTABLISHED 0          27675
tcp        0      0 127.0.0.1:42946         127.0.0.1:59983         ESTABLISHED 0          4441
tcp        0      0 127.0.0.1:50436         127.0.0.1:59503         ESTABLISHED 0          2697
tcp        0      0 127.0.0.1:50436         127.0.0.1:43906         ESTABLISHED 0          7121
tcp        0      0 127.0.0.1:50206         127.0.0.1:57027         ESTABLISHED 0          2678
tcp        0      0 127.0.0.1:33197         127.0.0.1:55264         ESTABLISHED 0          27676
tcp        0      0 127.0.0.1:29595         127.0.0.1:33590         ESTABLISHED 0          34884
```

```
tcp        0      0 127.0.0.1:57887         127.0.0.1:33197         ESTABLISHED 0          4432
tcp        0      0 127.0.0.1:36773         127.0.0.1:56441         ESTABLISHED 0          2641
tcp        0      0 127.0.0.1:57354         127.0.0.1:38841         ESTABLISHED 0          4265
tcp        0      0 127.0.0.1:29595         127.0.0.1:40818         ESTABLISHED 0          67021
tcp        0      0 127.0.0.1:29595         127.0.0.1:45889         ESTABLISHED 0          4288
tcp        0      0 127.0.0.1:45894         127.0.0.1:29595         ESTABLISHED 0          4412
tcp        0      0 127.0.0.1:57883         127.0.0.1:33197         ESTABLISHED 0          4413
tcp        0      0 127.0.0.1:29595         127.0.0.1:45836         ESTABLISHED 0          1323
tcp        0      0 127.0.0.1:35592         127.0.0.1:50436         ESTABLISHED 11         34907
tcp        0      0 127.0.0.1:29595         127.0.0.1:45881         ESTABLISHED 0          4259
tcp        0      0 127.0.0.1:45839         127.0.0.1:29595         ESTABLISHED 0          1469
tcp        0      0 127.0.0.1:59990         127.0.0.1:42946         ESTABLISHED 0          5128
tcp        0      0 127.0.0.1:45854         127.0.0.1:29595         ESTABLISHED 0          2578
tcp        0      0 127.0.0.1:29595         127.0.0.1:45860         ESTABLISHED 0          2632
tcp        0      0 10.10.50.150:22         10.10.50.16:42504       ESTABLISHED 0          6553
tcp        0      0 127.0.0.1:44104         127.0.0.1:43938         ESTABLISHED 0          1409
tcp        0      0 127.0.0.1:42946         127.0.0.1:59988         ESTABLISHED 0          4592
tcp        0      0 127.0.0.1:33590         127.0.0.1:29595         ESTABLISHED 11         34883
tcp        0      0 127.0.0.1:36916         127.0.0.1:51222         ESTABLISHED 0          2680
tcp        0      0 127.0.0.1:45841         127.0.0.1:29595         ESTABLISHED 0          1472
tcp        0      0 127.0.0.1:33197         127.0.0.1:57892         ESTABLISHED 0          4579
tcp        0      0 127.0.0.1:45889         127.0.0.1:29595         ESTABLISHED 0          4287
tcp        0      0 127.0.0.1:57019         127.0.0.1:50206         ESTABLISHED 0          2639
tcp        0      0 127.0.0.1:44239         127.0.0.1:36455         ESTABLISHED 0          2684
tcp        0      0 127.0.0.1:29595         127.0.0.1:45837         ESTABLISHED 0          1408
tcp        0      0 127.0.0.1:45848         127.0.0.1:29595         ESTABLISHED 0          1479
tcp        0      0 127.0.0.1:38492         127.0.0.1:39516         ESTABLISHED 0          2226
tcp        0      0 127.0.0.1:59953         127.0.0.1:42946         ESTABLISHED 0          2675
tcp        0      0 127.0.0.1:60034         127.0.0.1:53512         ESTABLISHED 0          2669
tcp        0      0 127.0.0.1:29595         127.0.0.1:45868         ESTABLISHED 0          2668
tcp        0      0 127.0.0.1:50206         127.0.0.1:57052         ESTABLISHED 0          4427
tcp        0      0 127.0.0.1:59983         127.0.0.1:42946         ESTABLISHED 0          4440
tcp        0      0 127.0.0.1:45861         127.0.0.1:29595         ESTABLISHED 0          2633
tcp        0      0 127.0.0.1:45837         127.0.0.1:29595         ESTABLISHED 0          1407
tcp        0      0 127.0.0.1:45893         127.0.0.1:29595         ESTABLISHED 0          4401
tcp        0      0 127.0.0.1:44251         127.0.0.1:36455         ESTABLISHED 0          4273
tcp        0      0 127.0.0.1:29595         127.0.0.1:45893         ESTABLISHED 0          4402
tcp        0      0 127.0.0.1:43938         127.0.0.1:44104         ESTABLISHED 0          1410
tcp        0      0 127.0.0.1:44136         127.0.0.1:43938         ESTABLISHED 0          2672
tcp        0      0 127.0.0.1:33197         127.0.0.1:57883         ESTABLISHED 0          4414
tcp        0      0 127.0.0.1:57037         127.0.0.1:50206         ESTABLISHED 0          4262
tcp        0      0 127.0.0.1:52988         127.0.0.1:47257         ESTABLISHED 0          4590
tcp        0      0 127.0.0.1:29595         127.0.0.1:45839         ESTABLISHED 0          1470
tcp        0      0 127.0.0.1:29595         127.0.0.1:48610         ESTABLISHED 0          7097
tcp        0      0 127.0.0.1:53208         127.0.0.1:35345         ESTABLISHED 0          4269
tcp        0      0 127.0.0.1:59949         127.0.0.1:42946         ESTABLISHED 0          2645
tcp        0      0 127.0.0.1:42946         127.0.0.1:59949         ESTABLISHED 0          2646
tcp        0      0 127.0.0.1:29595         127.0.0.1:45847         ESTABLISHED 0          1487
tcp        0      0 127.0.0.1:39517         127.0.0.1:38492         ESTABLISHED 0          2221
tcp        0      0 127.0.0.1:47252         127.0.0.1:52988         ESTABLISHED 0          4434
tcp        0      0 127.0.0.1:36902         127.0.0.1:51222         ESTABLISHED 0          2606
tcp        0      0 127.0.0.1:53512         127.0.0.1:43904         ESTABLISHED 0          67023
tcp        0      0 127.0.0.1:35345         127.0.0.1:53208         ESTABLISHED 0          4268
tcp        0      0 127.0.0.1:50206         127.0.0.1:57057         ESTABLISHED 0          4571
tcp        0      0 127.0.0.1:29595         127.0.0.1:45840         ESTABLISHED 0          1480
tcp        0      0 127.0.0.1:36359         127.0.0.1:50436         ESTABLISHED 11         67115
tcp        0      0 127.0.0.1:45881         127.0.0.1:29595         ESTABLISHED 0          4258
tcp        0      0 127.0.0.1:50206         127.0.0.1:57019         ESTABLISHED 0          2640
tcp        0      0 127.0.0.1:45862         127.0.0.1:29595         ESTABLISHED 0          2634
tcp        0      0 127.0.0.1:44705         127.0.0.1:53512         ESTABLISHED 11         34885
tcp        0      0 127.0.0.1:38492         127.0.0.1:39517         ESTABLISHED 0          2227
tcp        0      0 127.0.0.1:34256         127.0.0.1:55985         ESTABLISHED 0          4278
tcp        0      0 127.0.0.1:45846         127.0.0.1:29595         ESTABLISHED 0          1477
tcp        0      0 127.0.0.1:50206         127.0.0.1:57004         ESTABLISHED 0          2224
tcp        0      0 127.0.0.1:55985         127.0.0.1:34244         ESTABLISHED 0          2687
tcp        0      0 127.0.0.1:57027         127.0.0.1:50206         ESTABLISHED 0          2677
tcp        0      0 127.0.0.1:29595         127.0.0.1:45844         ESTABLISHED 0          1484
tcp        0      0 127.0.0.1:29595         127.0.0.1:45856         ESTABLISHED 0          2585
tcp        0      0 127.0.0.1:44992         127.0.0.1:36015         ESTABLISHED 11         34890
tcp        0      0 127.0.0.1:56441         127.0.0.1:36773         ESTABLISHED 0          2642
```

```
tcp        0      0 127.0.0.1:48610         127.0.0.1:29595         ESTABLISHED 11         7096
tcp        0      0 127.0.0.1:53208         127.0.0.1:35369         ESTABLISHED 0          5131
tcp        0      0 127.0.0.1:41248         127.0.0.1:33775         ESTABLISHED 0          2683
tcp        0      0 127.0.0.1:43906         127.0.0.1:50436         ESTABLISHED 11         7120
tcp        0      0 127.0.0.1:53208         127.0.0.1:35340         ESTABLISHED 0          4260
tcp        0      0 127.0.0.1:50436         127.0.0.1:36359         ESTABLISHED 0          67116
tcp        0      0 127.0.0.1:50206         127.0.0.1:57037         ESTABLISHED 0          4263
tcp        0      0 127.0.0.1:29595         127.0.0.1:45861         ESTABLISHED 0          2636
tcp        0      0 127.0.0.1:36015         127.0.0.1:44992         ESTABLISHED 0          34889
tcp        0      0 127.0.0.1:36455         127.0.0.1:44251         ESTABLISHED 0          4274
tcp        0      0 127.0.0.1:50436         127.0.0.1:59528         ESTABLISHED 0          4577
tcp        0      0 127.0.0.1:57010         127.0.0.1:50206         ESTABLISHED 0          2582
tcp        0      0 127.0.0.1:56564         127.0.0.1:46496         ESTABLISHED 0          2596
tcp        0      0 127.0.0.1:50206         127.0.0.1:57012         ESTABLISHED 0          2594
tcp        0      0 127.0.0.1:36455         127.0.0.1:44239         ESTABLISHED 0          2685
tcp        0      0 127.0.0.1:43938         127.0.0.1:44118         ESTABLISHED 0          2223
tcp        0      0 127.0.0.1:51222         127.0.0.1:36916         ESTABLISHED 0          2681
tcp        0      0 127.0.0.1:35369         127.0.0.1:53208         ESTABLISHED 0          5130
tcp        0      0 127.0.0.1:46496         127.0.0.1:56564         ESTABLISHED 0          2595
tcp        0      0 127.0.0.1:39592         127.0.0.1:46164         ESTABLISHED 0          2689
tcp        0      0 127.0.0.1:50206         127.0.0.1:57039         ESTABLISHED 0          4267
tcp        0      0 127.0.0.1:43279         127.0.0.1:47143         ESTABLISHED 0          4428
tcp        0      0 127.0.0.1:45845         127.0.0.1:29595         ESTABLISHED 0          1476
tcp        0      0 127.0.0.1:43904         127.0.0.1:53512         ESTABLISHED 11         67022
tcp        0      0 127.0.0.1:42946         127.0.0.1:59990         ESTABLISHED 0          5129
tcp        0      0 127.0.0.1:45844         127.0.0.1:29595         ESTABLISHED 0          1475
tcp        0      0 10.10.50.150:22         10.10.50.18:48041       ESTABLISHED 0          34818
tcp        0      0 127.0.0.1:57012         127.0.0.1:50206         ESTABLISHED 0          2593
tcp        0      0 127.0.0.1:51222         127.0.0.1:36902         ESTABLISHED 0          2607
tcp        0      0 127.0.0.1:57008         127.0.0.1:50206         ESTABLISHED 0          2225
tcp        0      0 10.10.50.150:22         10.10.50.16:42536       ESTABLISHED 0          66886
tcp        0      0 127.0.0.1:45860         127.0.0.1:29595         ESTABLISHED 0          2631
tcp        0      0 127.0.0.1:29595         127.0.0.1:45863         ESTABLISHED 0          2638
tcp        0      0 127.0.0.1:44132         127.0.0.1:43938         ESTABLISHED 0          2643
tcp        0      0 127.0.0.1:45868         127.0.0.1:29595         ESTABLISHED 0          2667
tcp        0      0 127.0.0.1:39516         127.0.0.1:38492         ESTABLISHED 0          2220
tcp        0      0 127.0.0.1:29595         127.0.0.1:45842         ESTABLISHED 0          1482
tcp        0      0 127.0.0.1:46164         127.0.0.1:39592         ESTABLISHED 0          2688
tcp        0      0 127.0.0.1:57895         127.0.0.1:33197         ESTABLISHED 0          4596
tcp        0      0 127.0.0.1:44859         127.0.0.1:53512         ESTABLISHED 11         7098
tcp        0      0 127.0.0.1:37210         127.0.0.1:41078         ESTABLISHED 0          4293
tcp        0      0 127.0.0.1:50206         127.0.0.1:57010         ESTABLISHED 0          2583
tcp        0      0 127.0.0.1:53512         127.0.0.1:44859         ESTABLISHED 0          7099
tcp        0      0 127.0.0.1:34260         127.0.0.1:55985         ESTABLISHED 0          4294
tcp        0      0 127.0.0.1:29595         127.0.0.1:45894         ESTABLISHED 0          4415
tcp        0      0 127.0.0.1:57892         127.0.0.1:33197         ESTABLISHED 0          4578
tcp        0      0 127.0.0.1:43938         127.0.0.1:44132         ESTABLISHED 0          2644
tcp        0      0 127.0.0.1:56961         127.0.0.1:34647         ESTABLISHED 11         7103
tcp        0      0 127.0.0.1:43938         127.0.0.1:44136         ESTABLISHED 0          2673
tcp        0      0 127.0.0.1:44086         127.0.0.1:54304         ESTABLISHED 11         67027
tcp        0      0 127.0.0.1:34244         127.0.0.1:55985         ESTABLISHED 0          2686
tcp        0      0 127.0.0.1:57057         127.0.0.1:50206         ESTABLISHED 0          4570
tcp        0      0 127.0.0.1:50436         127.0.0.1:35592         ESTABLISHED 0          35094
tcp        0      0 127.0.0.1:57052         127.0.0.1:50206         ESTABLISHED 0          4426
tcp        0      0 127.0.0.1:59988         127.0.0.1:42946         ESTABLISHED 0          4591
tcp        0      0 127.0.0.1:45836         127.0.0.1:29595         ESTABLISHED 0          1322
tcp        0      0 127.0.0.1:45843         127.0.0.1:29595         ESTABLISHED 0          1474
tcp        0      0 127.0.0.1:45842         127.0.0.1:29595         ESTABLISHED 0          1473
tcp        0      0 127.0.0.1:33197         127.0.0.1:57895         ESTABLISHED 0          4597
tcp        0      0 127.0.0.1:52988         127.0.0.1:47252         ESTABLISHED 0          4435
tcp        0      0 127.0.0.1:53512         127.0.0.1:44705         ESTABLISHED 0          34886
tcp        0      0 127.0.0.1:45840         127.0.0.1:29595         ESTABLISHED 0          1471
tcp        0      0 127.0.0.1:50206         127.0.0.1:57008         ESTABLISHED 0          2228
tcp        0      0 127.0.0.1:33787         127.0.0.1:41248         ESTABLISHED 0          4270
tcp        0      0 127.0.0.1:29595         127.0.0.1:45846         ESTABLISHED 0          1486
tcp        0      0 127.0.0.1:45879         127.0.0.1:29595         ESTABLISHED 0          4253
 --More--
```

run show system core-dumps

The **run show system core-dumps** command displays information about the system core files.

Command Syntax
run show system core-dumps

Example
• This example demonstrates how to show system core-dumps:

```
admin@XorPlus# run show system core-dumps
total 0
```

run show system cpu-usage

The **run show system cpu-usage** command displays information about the cpu usage.

Command Syntax
run show system cpu-usage

Example
• This example demonstrates how to show system connections:

```
admin@XorPlus# run show system cpu-usage
CPU usage: 7%
```

run show system date

The **run show system date** command displays information about the system current date.

Command Syntax
run show system date

Example
• This example demonstrates how to show system date:

```
admin@XorPlus# run show system date
Thu Nov 10 23:55:38 UTC 2005
```

run show system fan

The **run show system fan** command displays information about the system status of fan.

Command Syntax
run show system fan

Example
• This example demonstrates how to show system fan:

```
admin@XorPlus# run show system fan
Sensor Temperature:
Sensor 1 Temperature : 45 C / 113.00 F
Sensor 2 Temperature : 42 C / 107.60 F
Sensor 3 Temperature : 47 C / 116.60 F
Sensor 4 Temperature : 38 C / 100.40 F
Fan Status:
Fan 1 speed = 9747 RPM, PWM = 59, Forward
Fan 2 speed = 9836 RPM, PWM = 59, Forward
Fan 3 speed = 9782 RPM, PWM = 59, Forward
```

run show system memory-usage

The **run show system memory-usage** command displays information about memory usage.

Command Syntax
run show system memory-usage

Example
• This example demonstrates how to show system memory-usage:

```
admin@XorPlus# run show system memory-usage
total used free shared buffers cached
Mem: 515808 200528 315280 0 3048 60864
-/+ buffers/cache: 136616 379192
Swap: 0 0 0
```

run show system name

The **run show system name** command displays information about the host name.

Command Syntax
run show system name

Example
• This example demonstrates how to show system name:

```
admin@XorPlus# run show system name
admin@XorPlus
```

run show system ntp-status

The **run show system ntp-status** command displays information about the switch NTP status.

Command Syntax
run show system ntp-status

Example
• This example demonstrates how to show system ntp-status:

```
admin@XorPlus# run show system ntp-status
NTP Server information:
server 192.168.10.100
NTP Server Sync information:
ntp_gettime() returns code 0 (OK)
  time d709f74e.9b523000  Tue, Apr 29 2014 10:02:54.606, (.606723),
  maximum error 6016 us, estimated error 16 us, TAI offset 0
ntp_adjtime() returns code 0 (OK)
  modes 0x0 (),
  offset 0.000 us, frequency 0.000 ppm, interval 1 s,
  maximum error 6016 us, estimated error 16 us,
  status 0x1 (PLL),
  time constant 7, precision 1.000 us, tolerance 500 ppm,
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.168.10.100  .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

run show system os

The **run show system os** command displays information about operating system details.

Command Syntax
run show system os

Example
• This example demonstrates how to show system os:

```
admin@XorPlus# run show system os
Linux XorPlus 2.6.27 #1 Mon Mar 3 20:40:05 CST 2014 ppc GNU/Linux
```

run show system processes brief

The **run show system processes brief** command displays processes in a brief format.

Command Syntax
run show system processes brief

Example
• This example demonstrates how to show system processes succinctly:

```
admin@XorPlus# run show system processes brief
PID TTY STAT TIME COMMAND
1 ? Ss 0:01 init [2]
2 ? S< 0:00 [kthreadd]
3 ? S< 0:01 [ksoftirqd/0]
4 ? S< 0:00 [watchdog/0]
5 ? S< 0:14 [events/0]
6 ? S< 0:00 [khelper]
48 ? S< 0:00 [kblockd/0]
55 ? S< 0:00 [ata/0]
56 ? S< 0:00 [ata_aux]
58 ? S< 0:00 [kseriod]
99 ? S 0:00 [pdflush]
100 ? S 0:00 [pdflush]
101 ? S< 0:00 [kswapd0]
147 ? S< 0:00 [aio/0]
156 ? S< 0:00 [nfsiod]
831 ? S< 0:00 [ftld]
853 ? S< 0:00 [rpciod/0]
857 ? S< 0:00 [kjournald]
2338 ? Ss 0:00 /usr/sbin/cron -L 0
2370 ? Ss 0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
2483 ? S 0:18 pica_cardmgr
2485 ? S 6:14 pica_sif
2631 ? S 0:32 pica_lacp
2648 ? Sl 102:22 pica_lcmgr
2654 ? S 0:29 pica_login
3405 ? S 3:10 pica_mstp
3409 ? S 0:18 xorp_policy
3411 ? Ss 8:12 /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/run/xorp_rtrmgr.pid
3450 ? S 0:57 pica_dhcp
3466 ? S 0:36 xorp_static_routes
3474 ? S 0:37 xorp_ospfv2
3511 tty1 Ss+ 0:00 /sbin/getty 38400 tty1
3518 tty2 Ss+ 0:00 /sbin/getty 38400 tty2
3519 tty3 Ss+ 0:00 /sbin/getty 38400 tty3
3816 ? Ss 0:00 dhclient eth0
4880 ? Ss 0:00 in.telnetd: 10.10.50.47
4881 pts/0 Ss 0:00 login -h 10.10.50.47 -p
4882 pts/0 S+ 0:00 -bash
4891 pts/0 S+ 0:02 /pica/bin/pica_sh
9021 pts/0 R 0:00 ps ax
15109 ? Ss 0:00 in.telnetd: 10.10.50.47
15110 pts/1 Ss 0:00 login -h 10.10.50.47 -p
15111 pts/1 S+ 0:00 -bash
15120 pts/1 S+ 0:17 /pica/bin/pica_sh
15327 ? Ss 0:00 in.telnetd: 10.10.50.47
15328 pts/2 Ss 0:00 login -h 10.10.50.47 -p
15342 pts/2 S+ 0:00 -bash
15351 pts/2 S+ 0:26 /pica/bin/pica_sh
15869 ttyS0 Ss 0:00 /bin/login -
15870 ttyS0 S+ 0:00 -bash
15881 ttyS0 S+ 0:17 /pica/bin/pica_sh
21746 ? Ss 0:00 in.telnetd: 10.10.50.153
```

```
21747 pts/3 Ss 0:00 login -h 10.10.50.153 -p
21748 pts/3 S+ 0:00 -bash
21757 pts/3 S+ 0:10 /pica/bin/pica_sh
27523 ? Sl 0:00 /usr/sbin/rsyslogd -c5
31989 ? S 0:00 radvd
31990 ? Ss 0:01 radvd
```

run show system processes detail

The **run show system processes detail** command displays processes in a detailed format.

Command Syntax
run show system processes detail

Example
• This example demonstrates how to show system processes detail:

```
admin@XorPlus# run show system processes detail
USER   PID   %CPU   %MEM   VSZ   RSS   TTY   STAT  START   TIME    COMMAND
root   1      0.0   0.1   2400   856    ?     Ss   Nov09   0:01    init [2]
root   2      0.0   0.0    0      0     ?     S<   Nov09   0:00   [kthreadd]
root   3      0.0   0.0    0      0     ?     S<   Nov09   0:01   [ksoftirqd/0]
root   4      0.0   0.0    0      0     ?     S<   Nov09   0:00   [watchdog/0]
root   5      0.0   0.0    0      0     ?     S<   Nov09   0:14   [events/0]
root   6      0.0   0.0    0      0     ?     S<   Nov09   0:00   [khelper]
root   48     0.0   0.0    0      0     ?     S<   Nov09   0:00   [kblockd/0]
root   55     0.0   0.0    0      0     ?     S<   Nov09   0:00   [ata/0]
root   56     0.0   0.0    0      0     ?     S<   Nov09   0:00   [ata_aux]
root   58     0.0   0.0    0      0     ?     S<   Nov09   0:00   [kseriod]
root   99     0.0   0.0    0      0     ?     S    Nov09   0:00   [pdflush]
root   100    0.0   0.0    0      0     ?     S    Nov09   0:00   [pdflush]
root   101    0.0   0.0    0      0     ?     S<   Nov09   0:00   [kswapd0]
root   147    0.0   0.0    0      0     ?     S<   Nov09   0:00   [aio/0]
root   156    0.0   0.0    0      0     ?     S<   Nov09   0:00   [nfsiod]
root   831    0.0   0.0    0      0     ?     S<   Nov09   0:00   [ftld]
root   853    0.0   0.0    0      0     ?     S<   Nov09   0:00   [rpciod/0]
root   857    0.0   0.0    0      0     ?     S<   Nov09   0:00   [kjournald]
root   2338   0.0   0.1   2768   852    ?     Ss   Nov09   0:00   /usr/sbin/cron -L 0
root   2370   0.0   0.1   3656   1020   ?     Ss   Nov09   0:00   /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -st
root   2483   0.0   1.4   22660  7532   ?     S    Nov09   0:18   pica_cardmgr
root   2485   0.4   4.5   43000  23444  ?     S    Nov09   6:16   pica_sif
root   2631   0.0   1.6   26504  8620   ?     S    Nov09   0:32   pica_lacp
root   2648   6.6   5.6   108136 29188  ?     Sl   Nov09   103:00 pica_lcmgr
root   2654   0.0   2.4   30596  12688  ?     S    Nov09   0:30   pica_login
root   3405   0.2   2.7   32244  14200  ?     S    Nov09   3:11   pica_mstp
root   3409   0.0   1.3   18624  7100   ?     S    Nov09   0:18   xorp_policy
root   3411   0.5   3.4   40304  17772  ?     Ss   Nov09   8:16   /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/r
root   3450   0.0   1.8   27524  9488   ?     S    Nov09   0:58   pica_dhcp
root   3466   0.0   1.4   18060  7284   ?     S    Nov09   0:36   xorp_static_routes
root   3474   0.0   1.4   19816  7600   ?     S    Nov09   0:37   xorp_ospfv2
root   3511   0.0   0.1   2672   916    tty1  Ss+  Nov09   0:00   /sbin/getty 38400 tty1
root   3518   0.0   0.1   2672   916    tty2  Ss+  Nov09   0:00   /sbin/getty 38400 tty2
root   3519   0.0   0.1   2672   916    tty3  Ss+  Nov09   0:00   /sbin/getty 38400 tty3
root   3816   0.0   0.4   5128   2336   ?     Ss   Nov09   0:00   dhclient eth0
root   4880   0.0   0.2   2784   1084   ?     Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   4881   0.0   0.2   3492   1268   pts/0 Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  4882   0.0   0.2   3500   1544   pts/0 S+   Nov10   0:00   -bash
admin  4891   0.0   2.1   38396  11308  pts/0 S+   Nov10   0:02   /pica/bin/pica_sh
admin  9436   0.0   0.2   3208   1112   pts/0 R    00:31   0:00   ps aux
root   15109  0.0   0.2   2784   1084    ?    Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   15110  0.0   0.2   3492   1268   pts/1 Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  15111  0.0   0.2   3500   1544   pts/1 S+   Nov10   0:00   -bash
admin  15120  0.0   2.4   40068  12536  pts/1 S+   Nov10   0:17   /pica/bin/pica_sh
root   15327  0.0   0.2   2784   1092    ?    Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   15328  0.0   0.2   3492   1268   pts/2 Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  15342  0.0   0.2   3500   1544   pts/2 S+   Nov10   0:00   -bash
admin  15351  0.0   2.6   41480  13684  pts/2 S+   Nov10   0:27   /pica/bin/pica_sh
root   15869  0.0   0.2   3492   1268   ttyS0 Ss   Nov10   0:00   /bin/login -
admin  15870  0.0   0.3   3540   1696   ttyS0 S+   Nov10   0:00   -bash
admin  15881  0.0   2.6   41272  13908  ttyS0 S+   Nov10   0:17   /pica/bin/pica_sh
root   21746  0.0   0.2   2784   1084    ?    Ss   Nov10   0:00   in.telnetd: 10.10.50.153
```

```
root   21747  0.0   0.2   1268         pts/3  Ss   Nov10   0:00   login -h 10.10.50.153 -p
admin  21748  0.0   0.2   3500   1544  pts/3  S+   Nov10   0:00   -bash
admin  21757  0.0   2.2   39704  11652 pts/3  S+   Nov10   0:10   /pica/bin/pica_sh
root   27523  0.0   0.3   28488  1736   ?     Sl   Nov10   0:00   /usr/sbin/rsyslogd -c5
root   31989  0.0   0.0   2448   368    ?     S    Nov10   0:00   radvd
root   31990  0.0   0.0   2448   508    ?     Ss   Nov10   0:01   radvd
```

run show system rollback compare to

The **run show system rollback compare to** command shows the difference between tow rolled back configurations.

Command Syntax
run show system rollback compare to <other-config>

Parameter
•<other-config>Show the difference between rolled back configuration [1-49] and current configuration.

Example
• This example demonstrates how to show system rollback compare to 02:

```
admin@XorPlus# run show system rollback compare to 02
3c3
< /*Last commit     : Tue Apr 29 10:02:42 2014 by admin*/
---
> /*Last commit     : Tue Apr 29 09:38:47 2014 by admin*/
23c23
<             code-point 32
---
>             code-point 0
1254d1253
<     ntp-server-ip 192.168.10.100
```

run show system rollback file

The **run show system rollback file** command shows rolled back configuration file.

Command Syntax
run show system rollback file <rollback>

Parameter
•<other-config>Show rolled back configuration, range is [01, 02, 03, ... 49].

Example
• This example demonstrates how to show system rollback file 01:

```
admin@XorPlus# run show system rollback file 01
/*XORP Configuration File, v1.0*/
/* Copyright (C) 2009-2013 Pica8, Inc.*/
/*Last commit     : Fri Nov 11 15:17:55 2005 by root*/
/*PicOS Version   : 2.0.6*/
/*Version Checksum: 6165f4a04921d24410b9bf2780b0a960*/
interface {
    ecmp {
        max-path: 4
        hash-mapping {
            field {
                ingress-interface {
                    disable: true
                }
                vlan {
                    disable: true
                }
                ip-protocol {
                    disable: true
                }
                ip-source {
                    disable: false
                }
                ip-destination {
                    disable: false
                }
                port-source {
                    disable: false
                }
                port-destination {
                    disable: false
                }
            }
        }
    }
    aggregate-balancing {
        hash-mapping {
            field {
                ingress-interface {
                    disable: false
                }
                ethernet-source-address {
                    disable: false
                }
                ethernet-destination-address {
                    disable: false
                }
                ethernet-type {
                    disable: false
                }
                vlan {
```

```
                    disable: false
                }
                ip-protocol {
                    disable: false
                }
                ip-source {
                    disable: false
                }
                ip-destination {
                    disable: false
                }
                port-source {
                    disable: false
                }
                port-destination {
                    disable: false
                }
--More--
```

run show system rollback list

The **run show system rollback list** command shows rolled back file list.

Command Syntax
run show system rollback list

Example
• This example demonstrates how to show system rollback list:

```
admin@XorPlus# run show system rollback list
-rw-rw-r-- 1 admin xorp 14003 Nov 11 15:43 /pica/config/pica.conf
-rw-rw-r-- 1 admin xorp 14003 Nov 11 15:42 /pica/config/pica.conf.01
-rw-rw-r-- 1 root  xorp 13878 Nov 11 15:17 /pica/config/pica.conf.02
```

run show system rpsu

The **run show system rpsu** command shows the status of Redundant Power Supply Unit.

Command Syntax
run show system rpsu

Example
• This example demonstrates how to show system rpsu:

```
admin@XorPlus# run show system rpsu
RPSU is not supported for Pronto3290
```

run show system serial-number

The **run show system serial-number** command shows the serial number of Motherboard, RPSU, and SFP module.

Command Syntax
run show system serial-number

Example
• This example demonstrates how to show system serial-number:

```
admin@XorPlus# run show system serial-number

MotherBoard Serial Number : TW0WYGRVDNT0097I0015

RPSU 1 Serial Number      : N/A
RPSU 2: Not ready
SFP+    te-1/1/49             :
        Vendor Name           : Hisense
        Vendor PartNr         : LTF8502-BC+
        Serial Number         : CN56GMC2S0
        Module Type           : 10G_BASE_SR
        Cable Length          : 300m
SFP     te-1/1/50             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01408
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP     te-1/1/51             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01641
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP+    te-1/1/52             :
        Vendor Name           : 3M
        Vendor PartNr         : 1410-P17-00-3.00
        Serial Number         : Y30B220863
        Module Type           : 10G_BASE_AOC
        Cable Length          : 30m
```

run show system temperature

The **run show system temperature** command shows the switch temperature.

Command Syntax
run show system temperature

Example
• This example demonstrates how to show system temperature:

```
admin@XorPlus# run show system temperature
Temperature: 41 C / 105 F
```

run show system uptime

The **run show system uptime** command shows the time since system and processes started.

Command Syntax
run show system uptime

Example
• This example demonstrates how to show system uptime:

```
admin@XorPlus# run show system uptime
16:01:44 up 53 min, 3 users, load average: 0.09, 0.07, 0.09
```

run show system users

The **run show system users** command shows users who are currently logging in.

Command Syntax
run show system users

Example
• This example demonstrates how to show system users:

```
admin@XorPlus# run show system users
admin pts/0 Nov 11 15:35 (10.10.50.47)
admin ttyS0 Nov 11 15:18
admin pts/1 Nov 11 15:38 (10.10.50.47)
```

set system aaa local disable

The **set system aaa local disable** command enables the local authentication function.

Command Syntax
set system aaa local disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the local authentication function. The value is **true** or **false**. **true**: disables the local authentication function. **false**: enables the local authentication function. The default value is **false**.

Example
• Enable the local authentication function.

```
admin@XorPlus# set system aaa local disable true
admin@XorPlus# commit
```

set system aaa radius accounting disable

The **set system aaa radius accounting disable** command enables the RADIUS accounting function.

Command Syntax
set system aaa radius accounting disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the RADIUS accounting function. The value is **true** or **false**. **true**: disables the RADIUS accounting function. **false**: enables the RADIUS accounting function. The default value is **true**.

Example

• Enable the RADIUS accounting function.

```
admin@XorPlus# set system aaa radius accounting disable false
admin@XorPlus# commit
```

set system aaa radius accounting server-ip

The **set system aaa radius accounting server-ip** command configures IP address of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.

Example
- Configure IP address of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41
admin@XorPlus# commit
```

set system aaa radius accounting server-ip port

The **set system aaa radius accounting server-ip port** command configures port number of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*> **port** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
port <*integer*>	Specifies a port of a RADIUS accounting server. The value is an integer type. The default value is 1812. Note: The value of port number should be the same with that on the RADIUS servers.

Example
•Configure the port number of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 port 2
admin@XorPlus# commit
```

set system aaa radius accounting server-ip shared-key

The **set system aaa radius accounting server-ip shared-key** command configures shared key of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*> **shared-key** <*string*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
shared-key <*string*>	Specifies the shared key of RADIUS accounting server. The value is a string type. Note: The value of shared key should be the same with that on the RADIUS accounting servers.

Example
• Configure the shared key of RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 shared-key test123
admin@XorPlus# commit
```

set system aaa radius accounting server-ip timeout

The **set system aaa radius accounting server-ip timeout** command configures the response timeout interval of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*> **timeout** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
timeout <*integer*>	Specifies the response timeout interval of a RADIUS accounting server. When the NAS server sends a request message to the RADIUS accounting server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer in seconds. The default value is 5s.

Example
• Configure the response timeout interval of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 timeout 5
admin@XorPlus# commit
```

set system aaa radius authorization disable

The **set system aaa radius authorization disable** command enables the RADIUS authentication and authorization function.

Command Syntax
set system aaa radius authorization disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the RADIUS authentication and authorization function. The value is **true** or **false**. **true**: disables the RADIUS authentication and authorization function. **false**: enables the RADIUS authentication and authorization function. The default value is **true**.

Example
- Enable the RADIUS authentication and authorization function.

```
admin@XorPlus# set system aaa radius authorization disable false
admin@XorPlus# commit
```

set system aaa radius authorization server-ip

The **set system aaa radius authorization server-ip** command configures IP address of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.

Example
- Configure IP address of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41
admin@XorPlus# commit
```

set system aaa radius authorization server-ip port

The **set system aaa radius authorization server-ip port** command configures port number of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **port** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies the IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
port <*integer*>	Specifies a port of a RADIUS authentication and authorization server. The value is an integer type. The default value is 1812. Note: The value of port number should be the same with that on the RADIUS servers.

Example
- Configure the port number of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 port 2
admin@XorPlus# commit
```

set system aaa radius authorization server-ip shared-key

The **set system aaa radius authorization server-ip shared-key** command configures shared-key of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **shared-key** <*string*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
shared-key <*string*>	Specifies the shared key of RADIUS authentication and authorization server. The value is a string type. Note: The value of shared key should be the same with that on the RADIUS servers.

Example
• Configure the shared key of RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 shared-key test123
admin@XorPlus# commit
```

set system aaa radius authorization server-ip timeout

The **set system aaa radius authorization server-ip timeout** command configures the response timeout interval of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **timeout** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
timeout <*integer*>	Specifies the response timeout interval of a RADIUS authentication and authorization server. When the NAS server sends a request message to the RADIUS authentication and authorization server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer that ranges from 1 to 100, in seconds. The default value is 5s.

Example
- Configure the response timeout interval of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 timeout 10
admin@XorPlus# commit
```

set system aaa radius vrf mgmt-vrf

The **set system aaa radius vrf mgmt-vrf** command configures to run the AAA RADIUS protocol in management VRF.

Command Syntax

set system aaa radius vrf mgmt-vrf

Parameter

None.

Usage Guidelines

AAA RADIUS protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running AAA RADIUS protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the AAA RADIUS protocol to run in the management VRF.

```
admin@Xorplus# set system aaa radius vrf mgmt-vrf
admin@Xorplus# commit
```

set system aaa tacacs-plus accounting

The **set system aaa tacacs-plus accounting** command enables the TACACS+ accounting function.

Command Syntax
set system aaa tacacs-plus accounting <true | false>

Parameter

Parameter	Description
accounting <true | false>	Configures whether to enable or disable the TACACS+ accounting function. The value is **true** or **false**. **true**: enables the TACACS+ accounting function. It will take effect only when the TACACS+ function is enabled. **false**: disables the TACACS+ accounting function. The default value is **true**.

Example
- Enable the TACACS+ accounting function.

```
admin@XorPlus# set system aaa tacacs-plus accounting true
admin@XorPlus# commit
```

set system aaa tacacs-plus authorization

The **set system aaa tacacs-plus authorization** command enables the TACACS+ authorization function.

Command Syntax

set system aaa tacacs-plus authorization <**true | false**>

Parameter

Parameter	Description
authorization <true | false>	Configures whether to enable or disable the TACACS+ authorization function. The value is **true** or **false**. **true**: enables the TACACS+ authorization function. It will take effect only when the TACACS+ function is enabled. **false**: disables the TACACS+ authorization function. The default value is **true**.

Example

- Enable the TACACS+ authorization function.

```
admin@XorPlus# set system aaa tacacs-plus authorization true
admin@XorPlus# commit
```

set system aaa tacacs-plus auth-type

The **set system aaa tacacs-plus auth-type** command configures TACACS+ authentication type.

Command Syntax
set system aaa tacacs-plus auth-type <**ascii** | **chap** | **pap**>

Parameter

Parameter	Description
auth-type <ascii | chap | pap>	Specifies TACACS+ authentication type. The value could be **ascii**, **chap** or **pap**. The default value is **ascii**.

Example
- Configure TACACS+ authentication type.

```
admin@XorPlus# set system aaa tacacs-plus auth-type ascii
admin@XorPlus# commit
```

set system aaa tacacs-plus disable

The **set system aaa tacacs-plus disable** command enables the TACACS+ function.

Command Syntax

set system aaa tacacs-plus disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the TACACS+ function. The value is **true** or **false**. **true**: disables the TACACS+ function. **false**: enables the TACACS+ function. The default value is **true**.

Example

- Enable the TACACS+ function.

```
admin@XorPlus# set system aaa tacacs-plus disable false
admin@XorPlus# commit
```

set system aaa tacacs-plus key

The **set system aaa tacacs-plus key** command configures the shared key of TACACS+ server.

Command Syntax

set system aaa tacacs-plus key <*string*>

Parameter

Parameter	Description
key <*string*>	Specifies the shared key of TACACS+ server. The value is a string type. The default value is keystring. Note: The value of shared key should be the same with that on the TACACS+ servers.

Example

- Configure the shared key of TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus key pica8pica8
admin@XorPlus# commit
```

set system aaa tacacs-plus port-number

The **set system aaa tacacs-plus port-number** command configures the port number of a TACACS+ server.

Command Syntax
set system aaa tacacs-plus port-number <*integer*>

Parameter

Parameter	Description
port-number <*integer*>	Specifies a port of a TACACS+ server. The value is an integer type. The default value is 49. Note: The value of port number should be the same with that on the TACACS+ servers.

Example
- Configure the port number of a TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus port-number 3
admin@XorPlus# commit
```

set system aaa tacacs-plus timeout

The **set system aaa tacacs-plus timeout** command configures the response timeout interval of a TACACS+ server.

Command Syntax

set system aaa tacacs-plus timeout <*integer*>

Parameters

Parameter	Description
timeout <*integer*>	Specifies the response timeout interval of a TACACS+ server. When the NAS server sends a request message to the TACACS+ server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer in seconds. The default value is 5s.

Example

- Configure the response timeout interval of a TACACS+ server.

```
admin@Xorplus# set system aaa tacacs-plus timeout 30
```

set system aaa tacacs-plus server-ip

The **set system aaa tacacs-plus server-ip** command configures IP address of a TACACS+ server.

Command Syntax
set system aaa tacacs-plus server-ip <*ipv4_address*>

Parameter

Parameter	Description
server-ip <*ipv4_address*>	Specifies IP address of a TACACS+ server. The value is in dotted decimal notation.

Usage Guidelines

PicOS supports a maximum of eight TACACS+ servers. When multiple TACACS+ servers are configured, only one will be used, the IP addresses are used in alphabetical order.

For example, the following TACACS+ servers are configured.

```
set system aaa tacacs-plus server-ip 146.13.191.77
set system aaa tacacs-plus server-ip 146.13.191.78
set system aaa tacacs-plus server-ip 1.1.1.1
set system aaa tacacs-plus server-ip 2.2.2.2
set system aaa tacacs-plus server-ip 3.3.3.3
```

The servers will be used in below order.

1. 1.1.1.1
2. 146.13.191.77
3. 146.13.191.78
4. 2.2.2.2
5. 3.3.3.3

Example

- Configure IP address of a TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus server-ip 10.10.53.53
admin@XorPlus# commit
```

set system aaa tacacs-plus source-interface

The **set system aaa tacacs-plus source-interface** command sets the source interface the switch uses to connect to the TACACS+ server.

Command Syntax

set system aaa tacacs-plus source-interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the source interface. The value could be an L3 VLAN interface, loopback interface, routed interface or sub-interface that enabled inband management or eth0. By default, the source interface is eth0.

Usage Guidelines

NOTE:

- When using a L3 VLAN interface, loopback interface, routed interface or sub-interface as a source interface connecting to the TACACS+ server, you have to enable inband management function by using commands **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.
- Remember to specify an IP address for the source interface.

Example

- Set the source interface the switch uses to connect to the server to loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.1.1.1 prefix-length 32
admin@Xorplus# set system aaa tacacs-plus source-interface loopback
```

- Set the source interface the switch uses to connect to the server to L3 VLAN interface.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 100
admin@Xorplus# set l3-interface vlan-interface vlan100 address 10.10.51.129 prefix-length 24
admin@Xorplus# set vlans vlan-id 100 l3-interface vlan100
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# set system aaa tacacs-plus source-interface vlan100
```

set system aaa local-auth-fallback disable

The **set system aaa local-auth-fallback disable** command is used to enable or disable the local authentication fallback function.

Command Syntax

set system aaa local-auth-fallback disable <**true | false**>

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable the local authentication fallback function. The value could be **true** or **false**. • **true**: disables the local authentication fallback function. • **false**: enables the local authentication fallback function. By default, the local authentication fallback function is disabled.

Usage Guidelines

For management port or in-band interface login, if the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, the system determines whether to perform local authentication based on the configuration of local authentication fallback function,

- If the local authentication fallback function is enabled, then user will fallback to local authentication.
- If the local authentication fallback function is disabled, then the system generates a syslog message and user is denied access to local authentication.

NOTE:

- The local authentication fallback function is only applied to management port or in-band login interface in situations where the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available.
- The **set system aaa local-auth-fallback disable** <**true | false**> command does not applied to console login. For console login, if the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, the system generates a syslog and uses local user/passwd file for authentication. After successful login, local authorization will be performed.

Example

- Enable local authentication fallback function.

```
admin@Xorplus# set system aaa local-auth-fallback disable false
admin@Xorplus# commit
```

set system aaa tacacs-plus vrf mgmt-vrf

The **set system aaa tacacs-plus vrf mgmt-vrf** command configures to run the AAA TACACS+ protocol in management VRF.

Command Syntax

set system tacacs-plus radius vrf mgmt-vrf

Parameter

None.

Usage Guidelines

AAA TACACS+ protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running AAA TACACS+ protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the AAA TACACS+ protocol to run in the management VRF.

```
admin@Xorplus# set system aaa radius vrf mgmt-vrf
admin@Xorplus# commit
```

set system hostname

To specify or modify the hostname for the switch, use the **set system hostname** command in L2/L3 configuration mode. To reset the hostname to default, use the **delete** form of this command.

Command Syntax

set system hostname *hostname*
delete system hostname

Parameters

hostname	New hostname for the switch. The maximum length is 63.

Example

This example demonstrates how to configure the system's network name to 123.

```
admin@Switch# set system hostname 123
admin@Switch# commit
Commit OK.
Save done.
admin@123#
```

set system inband vlan-interface

The **set system inband vlan-interface** command sets a specified L3 VLAN interface in the default VRF as the inband management port.

Command Syntax

set system inband vlan-interface <*vlan-interface*>

Parameter

Parameter	Description
vlan-interface <*vlan-interface*>	Enables inband management on a specfied L3 VLAN interface in the default VRF. The value is a string.

Usage Guidelines

By default, the user cannot remotely log in and manage the switch through the L3 VLAN interface.

Use this command to set a specified L3 VLAN interface in the default VRF as the inband management port. The L3 VLAN interface with the inband management function enabled can transmit both management traffic and data plane traffic.

NOTE:

Only the L3 VLAN interface in the default VRF can be set as the inband management port. If a VLAN interface has been set as an inband management port, it cannot be bound to other user-defined VRFs.

Example

- Enable the inband management function of the L3 VLAN interface vlan100.

```
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# commit
```

set system inband loopback

The **set system inband loopback** command sets the loopback interface IP in the default VRF as the inband management IP.

Command Syntax

set system inband loopback <*ip-address*>

Parameter

Parameter	Description
loopback <*ip-address*>	Specifies the loopback interface IP in the default VRF as the inband management IP. The value could be an IPv4 or IPv6 address.

Example

- Enable the inband management function of the loopback interface.

```
admin@Xorplus# set system inband loopback 192.168.100.1
admin@Xorplus# commit
```

set system inband routed-interface

The **set system inband routed-interface** command sets a specified routed interface or sub-interface in the default VRF as the inband management port.

Command Syntax

set system inband routed-interface <*routed-interface*>

Parameter

Parameter	Description
routed-interface <*routed-interface*>	Enables inband management on a specfied routed interface or sub-interface in the default VRF. The value is a string.

Usage Guidelines

By default, the user cannot remotely log in and manage the switch through the routed interface or sub-interface.

Use this command to set a specified routed interface or sub-interface in the default VRF as the inband management port. The routed interface or sub-interface with the inband management function enabled can transmit both management traffic and data plane traffic.

NOTE:

Only the routed interface or sub-interface in the default VRF can be set as the inband management port. If a routed interface or sub-interface has been set as an inband management port, it cannot be bound to other user-defined VRFs.

Example

- Enable the inband management function of the routed interface.

```
admin@Xorplus# set system inband routed-interface rif-te1
admin@Xorplus# commit
```

set system inband enable

> **Warning:**
> The command **set system inband enable true** is obsolete and replaced by command **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.

The **set system inband enable** command is used to enable or disable the inband management function for all the L3 interfaces in the default VRF.

Command Syntax

set system inband enable <**true | false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enables or disables the inband management function for all the L3 interfaces in the default VRF. The value could be **true** or **false**. • **true**: enables the inband management function for all the L3 interfaces in the default VRF. • **false**: disables the inband management function for all the L3 interfaces in the default VRF. By default, inband management function is disabled.

Example

- Enable the inband management function for all the L3 interfaces in the default VRF.

```
admin@XorPlus# set system inband enable true
admin@XorPlus# commit
```

system login-acl network

User can configure the ACL to control whether remote hosts within specified subnetworks are allowed to log in the system. User can set ipv4-address/netmask or ipv6-address/netmask to configure remote hosts from both subnetworks log in. User can also delete them.

Command Syntax
set system login-acl network <*IPV4Net*>
set system login-acl network <*IPV6Net*>
delete system login-acl network <*IPV4Net*>
delete system login-acl network <*IPV6Net*>

Parameter
• <*IPV4Net*> It stands ipv4 address and netmask.
• <*IPV6Net*> It stands ipv6 address and netmask.

Example
• This example demonstrates how to configure the login ACL attributes is ipv4-address and netmask:

```
admin@XorPlus# set system login-acl network 192.168.1.0/24
admin@XorPlus# commit
```

• This example demonstrates how to configure the login ACL attributes is ipv6-address and netmask:

```
admin@XorPlus# set system login-acl network 2001:1:1:1::/64
admin@XorPlus# commit
```

system login announcement

User can configure a system announcement message (displayed after login).

Command Syntax
set system login announcement <*text*>
delete system login announcement

Parameter
• <*text*> VLAN tag identifier. The effective value type is text.

Example
• This example demonstrates how to configure the system announcement message after login:

```
admin@XorPlus# set system login announcement "welcome the switch-1101"
admin@XorPlus# commit
```

system login user

To configure a user account, use the **set system login user** command in L2/L3 configuration mode. To remove a user account, use the **delete** form of the command.

Command Syntax

set system login user *username*
delete system login user *username*

Parameter

username	The username for the new user.

Example

This example demonstrates how to create a new user account named pica8:

```
admin@Switch# set system login user pica8
```

system login user admin class

User can configure the user admin is a read-only account. The newly created user account, by default, is read-only.

Command Syntax
set system login user admin class <limit>
delete system login user admin class
Parameter
<*limit*> Configure the permission as read-only or super-user. Required select include:

- **read-only** permissions[view]
- **super-user** permission[all]
- Default value: read-only

Example
• This example demonstrates how to configure the user admin as super-user:

```
admin@XorPlus# set system login user admin class super-user
admin@XorPlus# commit
```

set system login user authentication plain-text-password

To create the password for a user account, use the **set system login user authentication plain-text-password** command in L2/L3 configuration mode. To remove the password for a user, use the delete form of the command.

NOTE: The encryption algorithm used to save user password to local is **MD5**.

Command Syntax

set system login user <*username*> **authentication plain-text-password** <*password*>
delete system login user <*username*> **authentication plain-text-password**

Parameters

Parameter	Description
user <*username*>	Name of user. The value is a string.
plain-text-password <*password*>	User's password. The value is a string that must be at least 6 characters. The password can support the below complexity: 1. Lowercase letters a-z. 2. Uppercase letters A-Z. 3. Numerics (0, 1, 2, etc.) 4. Special Characters (@, %, !, etc.)

Example

- The following example sets the password for user **alpha**; if the username does not already exist, the command will also create it.

```
admin@Switch# set system login user alpha authentication plain-text-password mypica8
 admin@XorPlus# commit
```

- This example demonstrates how to create a password for the user **admin**:

```
admin@XorPlus# set system login user admin authentication plain-text-password pica8pica8
admin@XorPlus# commit
```

system login user class

To set permissions for a user, use the **system login user class** command in L2/L3 configuration mode. By default, a newly created user account is **read-only**. To delete a user, use the **delete** form of the command.

Command Syntax

set system login user *username* **class** [**read-only** | **super-user**]
delete system login user *username* **class**

Parameters

username	The name of the user.
read-only	(Optional) This keyword gives view-only or read-only permissions to user. This is the default option.
super-user	(Optional) This keyword gives all permissions to user. The default option is **read-only**.

Example

The following example configures a **super-user** account named alpha:

```
admin@Switch# set system login user alpha class super-user
```

set system timezone

User can configure local time zone or delete it.

Command Syntax
set system timezone <*time-zone*>
delete system timezone

Parameter
•<*time-zone*>The effective value is a time zone.

Example
• This example demonstrates how to set local time zone to Shanghai:

```
admin@XorPlus# set system timezone Asia/Shanghai
admin@XorPlus# commit
```

set system ntp server-ip

The **set system ntp server-ip** command configures the IP address of the remote NTP server.

Note: the route between NTP server and NTP source interface is required to be reachable.

Command Syntax

set system ntp server-ip *<ipv4-address>*

Parameter

Parameter	Description
server-ip *<ipv4-address>*	Specifies the IPv4 address of the remote server. The value is an IPv4 address, e.g. 192.168.10.100.

Example

- Configure the IP address of the remote NTP server.

```
admin@XorPlus# set system ntp server-ip 192.168.10.100
admin@XorPlus# commit
```

set system ntp source-interface

The **set system ntp source-interface** command configures the local source interface that sends NTP packets.

Command Syntax

set system ntp source-interface <*source-interface*>

Parameter

Parameter	Description
source-interface <*vlan-interface*>	Specifies the NTP source interface. The value could be **eth0**, L3 VLAN interface, loopback interface, routed interface or sub-interface. Indicates the local interface that sends the NTP packets.

Usage Guidelines

Configure the local source interface for sending/receiving NTP packets, so that the IP address of another interface on the device cannot be used as the destination address of a reply packet, which is convenient for a user to subsequently deploy a flow control policy.

Notes:

- If the NTP source interface is configured, the source interface will be used for the NTP connection.
- If the user defined VRF is configured, and NTP is enabled (in default VRF or management VRF) without configuring the NTP source interface, the system will continuously print an error syslog like the following.

> *Apr 13 2021 15:05:47 Xorplus daemon.info : failed to init interface for address 22.1.1.201*
>
> *Apr 13 2021 15:10:47 Xorplus daemon.err : bind(41) AF_INET 21.1.1.201#123 flags 0x19 failed: Cannot assign requested address*

Example

- Configure the local source interface that sends NTP packets.

```
admin@Xorplus# set system ntp source-interface vlan100
admin@Xorplus# commit
```

set system ntp vrf mgmt-vrf

The **set system ntp vrf mgmt-vrf** command configures to run the NTP protocol inmanagement VRF.

Command Syntax

set system ntp vrf mgmt-vrf

Parameter

None.

Usage Guidelines

NTP protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding NTP server is required to be route reachable in the VRF running NTP protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the NTP protocol to run in the management VRF.

```
admin@Xorplus# set system syslog vrf mgmt-vrf
admin@Xorplus# commit
```

set interface gigabit-ethernet ptp mode

The **set interface gigabit-ethernet ptp mode** command configures the device interface as the E2ETC node type, and enables the PTP function on the interface.

Command Syntax

set interface gigabit-ethernet <*port*> **ptp mode** {e2etransparent | none}

Parameter

Parameter	Description
port	Ethernet switching port identifier, the valid ports range: 1-52.
ptp mode {e2etransparent | none}	Configure the PTP mode on a switch interface: • e2etransparent: configures the device interface as the E2ETC node type and enables the PTP function on the interface. • none: disable the PTP function on the interface.

Note: the PTP function can only be configured on the physical interface.

Example

• Configure the port te-1/1/25 that receiving PTP messages and the port te-1/1/26 that sends PTP packets as E2ETC node.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/25 ptp mode e2etransparent
admin@Xorplus# set interface gigabit-ethernet te-1/1/26 ptp mode e2etransparent
```

set system services ssh connection-limit

The **set system services ssh connection-limit** command configures the SSH connection limit per source IP address.

Command Syntax
set system services ssh connection-limit <*int*>
delete system services ssh connection-limit

Parameter
• <*int*> It is the maximum number of allowed connections,the valid number range 0-250. Default value is 20.

Example
• This example demonstrates how to configure the SSH maximum number of connections as 5:

```
admin@XorPlus# set system services ssh connection-limit 5
admin@XorPlus# commit
```

set system services ssh disable

The set system services ssh disable command configures the permission of the SSH login.

Command Syntax
set system services ssh disable <*bool*>
delete system services ssh disable

Parameter
•<*bool*> The effective value is **true** or **false**. If the value is true, SSH login is disabled. If value is false, SSH login is enabled.

Example
• This example demonstrates how to configure SSH login as permission:

```
admin@XorPlus# set system services ssh disable false
admin@XorPlus# commit
```

set system services ssh protocol-version v2

This command refers to which specific ssh protocol version is supported. User can configure it or delete it.

Command Syntax
set system services ssh protocol-version v2
delete system services ssh protocol-version

Example
• This example demonstrates how to set the specific ssh protocol versions supported to v2:

```
admin@XorPlus# set system services ssh protocol-version v2
admin@XorPlus# commit
```

set system services ssh rate-limit

User can configure the maximum number of connections per minute and per source IP address or delete the configuration.

Command Syntax
set system services ssh rate-limit <*int*>
delete system services ssh rate-limit

Parameter
•<*int*> The effective value type is int. The valid number range 1-20.

Example
• This example demonstrates how to set the maximum number of connections per minute to 2:

```
admin@XorPlus# set system services ssh rate-limit 2
admin@XorPlus# commit
```

set system services ssh root-login

User can configure allow or deny root access via ssh or delete the limits of authority.

Command Syntax
set system services ssh root-login <*limit*>
delete system services ssh root-login

Parameter
• <*limit*> Configure allow or deny root access via ssh. Required select include:

- **allow** allow root access via ssh
- **deny** do not allow root access via ssh

Example
• This example demonstrates how to allow the root access via ssh:

```
admin@XorPlus# set system services ssh root-login allow
admin@XorPlus# commit
```

set system services ssh idle-timeout

The **set system services ssh idle-timeout** command configures the idle timeout for SSH connections.

Command Syntax

set system services ssh idle-timeout <*timeout-value*>

Parameter

Parameter	Description
idle-timeout <*timeout-value*>	Specifies the idle timeout for SSH connections. The value is an integer, in minutes, that ranges from 0 to 20000. The default value is 0, which means no idle timeout for SSH user.

Usage Guidelines

If the SSH user logs in to the system but doesn't perform any for a long time, the SSH channel resources would be occupied for a long time thus making it difficult or impossible for other users to log in to the system. The SSH idle timeout duration is configured to release SSH resources in time. The SSH connection will be automatically disconnected if the SSH user who logged in to the system doesn't perform any operation within the SSH idle timeout duration. The following disconnect prompt is printed:

Connection to 10.10.51.193 closed by remote host.

Connection to 10.10.51.193 closed.

NOTE:

- The idle timeout timer is restarted each time the SSH user perform an operation.
- The configuration takes effect only on the next SSH login.
- The same idle timeout value is available for all the SSH users.

Example

- Configure the idle timeout for SSH user to 60 minutes.

```
admin@Xorplus# set system services ssh idle-timeout 60
```

set system services ssh port

The **set system services ssh port** command changes the listening port number of the SSH server.

Command Syntax

set system services ssh port *<port-number>*

Parameter

Parameter	Description
port *<port-number>*	Specifies the listening port number of the SSH server. The value is an integer ranging from 1 to 65535. The default listening port number of the SSH server is 22.

Usage Guidelines

Users can use this command to configure the new port number of SSH server to prevent attackers from accessing the standard port of SSH service and ensure security.

Note that,

If the modified port number is not 22, the client needs to specify port number when logging in using SSH.

Example

- Change the listening port number of the SSH server to 30.

```
admin@Xorplus# set system services ssh port 30
admin@Xorplus# commit
```

set system snmp-acl security-name network

The **set system snmp-acl security-name network** command configures SNMP access control white list.

Command Syntax

set system snmp-acl [**security-name** <*community-name*>] **network** <*ip/mask*>

Parameter

Parameter	Description
security-name <*community-name*>	Optional. Specifies the name of a community. The value is a string. It is a **community name** for SNMPv1/SNMPv2, **security name** for SNMPv3.
network <*ip/mask*>	Specifies the network where the SNMP queries come from. The format is *IPv4/mask or IPv6/mask*. For example, 10.10.10.0/24.

Usage Guidelines

SNMP ACL has two types of access control white list: As-per User List and Global List.

- As-per User List

The SNMP ACL that specifies a security name can be configured with multiple networks and is called the as-per user list. For example,

```
admin@XorPlus# set system snmp-acl security-name public network 10.10.50.0/24
```

Where "security-name" is the **community name** for SNMPv1 and SNMPv2, and the **security name** for SNMPv3.

- Global List

SNMP ACLs that do not specify a security name but only networks are called the global list. For example,

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl network 10.10.51.0/24
```

The global list is applied to NMS that are not configured with an as-per user list.

NOTE:

- Multiple as-per user lists of different networks can be configured under one security name.
- If an SNMP ACL with security name is configured, but no network list is configured under this security name, this as-per user list is empty and invalid, then global list matching will be performed.

Example

- Configure an SNMP ACL as-per user list, NMS with the security name **public** and from network 10.10.50.0/24 can access the device.

```
admin@XorPlus# set system snmp-acl security-name public network 10.10.50.0/24
admin@XorPlus# commit
```

- Configure an SNMP ACL global list, NMS from 192.168.10.0/24 can access the device.

```
admin@XorPlus# set system snmp-acl network 192.168.10.0/24
admin@XorPlus# commit
```

set system syslog server-ip

The **set system syslog server-ip** command configures the remote syslog server on the switch, including IP address, port number, transmission protocol and source interface. After user configures the syslog server IP address, the log files will be sent to the syslog server.

The **delete system syslog server-ip** command deletes the configuration of remote syslog server.

Command Syntax
set system syslog server-ip <*ip_address*> [**port** <*port_number*> | **protocol** <**tcp | udp**> | **source-interface** <*source-interface*>]

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of a remote syslog server. It could be an IPv4 address or IPv6 address.
port <*port_number*>	Optional. Specifies the port of the remote syslog server. The value is an integer type.
protocol <**tcp	udp**>	Optional. Specifies the transmission protocol for the remote syslog server. The value could be **tcp** or **udp**.
source-interface <*source-interface*>	Optional. Specifies the source interface for sending/receiving syslog messages, e.g. vlan20, eth0, routed interface, sub-interface or loopback.

Notes:

- The IP address of the source interface will be used as the source IP in the IP header after syslog message is routed.
- If syslog uses **TCP** protocol, source-interface can't be configured at the same time.

Example
• This example configures how to set the IP address of the remote syslog server.

```
admin@XorPlus# set system syslog server-ip 192.168.1.1
admin@XorPlus# commit
```

set system syslog local-file

The **set system syslog local-file** command sets the local save location of the syslog file.

Command Syntax

set system syslog local-file *<location>*

Parameter

Parameter	Description
local-file *<location>*	Specifies the local save location of the syslog. The value could be **disk** or **ram**. • **disk**: saves the syslog to disk, the path is /var/log. • **ram**: saves the syslog to RAM, the path is /tmp/log. By default, the syslog is kept in RAM.

Usage Guidelines

By default, the syslog file stays in RAM. When the system is powered off and restarted, the syslog file in RAM will be cleared. You can configure the syslog to be saved to disk. When the system is powered off and restarted, the syslog saved to disk will still exist.

Example

- Set the local save location of the syslog file to disk.

```
admin@XorPlus# set system syslog local-file disk
admin@XorPlus# commit
```

set system syslog vrf mgmt-vrf

The **set system syslog vrf mgmt-vrf** command configures to run the syslog service in management VRF.

Command Syntax

set system syslog vrf mgmt-vrf

Parameter

None.

Usage Guidelines

Syslog service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding syslog server is required to be route reachable in the VRF running syslog service.

Note: The latest configuration overrides the previous one.

Example

- Configure the syslog service to run in the management VRF.

```
admin@Xorplus# set system syslog vrf mgmt-vrf
admin@Xorplus# commit
```

set system usb disable

The **set system usb disable** command configures whether to disable all external USB interfaces of the switch.

Command Syntax

set system usb disable [**true | false**]

Parameter

Parameter	Description
disable [**true	false**]	Configures whether to disable the USB interfaces. The value is **true** or **false**. **true**: disables the USB interface. **false**: enables the USB interface. The default value is **false**.

Example

- Disable the USB interfaces.

```
admin@Xorplus# set system usb disable true
admin@Xorplus# commit
```

- Enable the USB interfaces.

```
admin@Xorplus# set system usb disable false
admin@Xorplus# commit
```

set system management-ethernet eth0 ip-address {IPv4 | IPv6}

The **set system management-ethernet eth0 ip-address** {**IPv4** | **IPv6**} command sets a static IP address for management interface eth0.

Command Syntax

set system management-ethernet eth0 ip-address {**IPv4** | **IPv6**} <*ip_address*>

Parameter

Parameter	Description
{**IPv4** | **IPv6**} <*ip_address*>	Specifies the IP address for management interface eth0. When assigning an IPv4 address, the value is in dotted decimal notation. When assigning an IPv6 address, the value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers.

Example

- Set the IP address 192.168.10.5/24 for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-address IPv4 192.168.10.5/24
admin@Xorplus# commit
```

set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}

The **set system management-ethernet eth0 ip-gateway** {**IPv4** | **IPv6**} command sets the gateway address for management interface eth0.

Command Syntax

set system management-ethernet eth0 ip-gateway {**IPv4** | **IPv6}** <*ip_address*>

Parameter

Parameter	Description
{**IPv4** | **IPv6}** <*ip_address*>	Specifies the gateway address for management interface eth0. For IPv4 address, the value is in dotted decimal notation. For IPv6 address, the value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers.

Example

- Set the gateway address 192.168.10.1 for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-gateway IPv4 192.168.10.1
admin@Xorplus# commit
```

show system management-ethernet

The **show system management-ethernet** command shows the configuration information, status and traffic statistics information of the management interface.

Command Syntax

show system management-ethernet

Parameter

None.

Example

- Run **run show system management-ethernet** command to view the configuration information, status and traffic statistics information of the management interface.

```
admin@Xorplus# run show system management-ethernet
eth0    Hwaddr: 68:21:5f:7f:10:c5       State: UP
        Gateway  : 192.168.10.1
        Inet addr:
                  192.168.10.5/24
                  fe80::6a21:5fff:fe7f:10c5/64
    Traffic statistics
        Input Packets.....................222156
        Input Bytes.......................13775674
        Output Packets.....................1471
        Output Bytes.......................140558

eth1    Hwaddr: 68:21:5f:7f:10:c9       State: UP
        Inet addr:
                  fe80::6a21:5fff:fe7f:10c9/64
    Traffic statistics
        Input Packets.....................0
        Input Bytes.......................0
        Output Packets.....................63
        Output Bytes......................4546
```

run request system reboot

The **run request system reboot** command restarts the device.

Command Syntax

run request system reboot *<description>*

Parameters

Parameter	Description
<description>	Optional. Add a description in the syslog before the system reboots by using **run request system reboot** command. The value is a string. If the description contains spaces, we need to enclose the whole string in double quotes.

Usage Guidelines

The command enables you to restart the device remotely.

After executing the reboot command, PICOS will automatically save the user configuration and restart the device with system diagnostics.

As system reboot will cause service interruption, so be cautious to use this command.

By configuring the description parameter, the system prints a system log with this description information before the system reboots.

- The log message containing this description is in the syslog file */var/log/messages*.
- The log message containing this description information is at the info level. To display the log message, you need to set the log-level to info or trace. Otherwise, the system will not record this log.
- The log message containing this description information is recorded only in the scenarios when the system is restarted by using run request system reboot *<description>* command. But in the scenarios of restarting the system when manually powered off or device fault, the system will not record the log message containing this description information.

Example

- Reboot PICOS.

```
admin@Xorplus# run request system reboot
```

- Reboot PICOS with the description information “Hello World”.

```
admin@Xorplus# set system syslog local-file disk   // Set the system log file to save to disk.
admin@Xorplus# run request system reboot "Hello World"
admin@Xorplus:~$ tail -f /var/log/messages       // Check the system logs.
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 1 plug in.
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 1 power on
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]rpsu 2 status changed from PSU_STATUS_INVALID to PSU_STATUS_PI
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 2 plug in.
Jan  3 1970 01:09:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:10:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:11:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:11:59 Xorplus auth.info : Accepted password for admin from 10.10.50.143 port 58420 ssh2
Jan  3 1970 01:12:10 Xorplus auth.info : Accepted password for admin from 10.10.50.143 port 58422 ssh2
Jan  3 1970 01:12:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:13:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:14:21 Xorplus local0.info : [LOGIN]Hello World  //The user configured reboot description log.

Broadcast message from root@Xorplus (Sat Jan  3 01:14:21 1970):


The system is going down for reboot NOW!


Broadcast message from root@Xorplus (Sat Jan  3 01:14:22 1970):


The system is going down for reboot NOW!
Jan  3 1970 01:14:22 Xorplus user.notice : shutting down for system reboot
[ ok  [....] Stopping internet superserver: inetd.
```

```
[ ok ] Stopping: L2/L3.............
[ ok ] Asking all remaining processes to terminate...done.
[ ok ] All processes ended within 1 seconds...done.
[ ok ] Stopping enhanced syslogd: rsyslogd.
[....] Deconfiguring network interfaces...Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
```

run show system hwinfo

The **run show system hwinfo** command displays the hardware information of PICOS switch.

Command Syntax

run show system hwinfo

Parameter

None.

Exampe

- Display the hardware information of PICOS switch.

```
admin@Xorplus# run show system hwinfo
Product Name: N3208PX-ON
Part Number: 0JDFTF
Serial Number: CN0JDFTFDND0083M0100
Base MAC Address: 20:04:0F:01:63:47
Manufacture Date: 02/22/2020 14:50:07
Device Version: 1
Label Revision: A00
Platform Name: armv7a-dellemc_n3208px_iproc-r0
Loader Version: 4.39.1.0-4
MAC Addresses: 128
Manufacturer: DND00
Country Code: CN
Vendor Name: Dell EMC
Diag Version: 4.39.3.0-1
Service Tag: 8VMGXC2
Vendor Extension: 0x00 0x00 0x02 0xA2
CRC-32: 0x4260903C(Valid)


admin@Xorplus# run show system hwinfo service-tag
Service Tag: 8VMGXC2
```

ping

The **ping** command is a method for troubleshooting the accessibility of devices and outputs the statistics results.

NOTE:

When ping a link-local address, the outband VLAN interface must be specified together, otherwise it will result link unreachable.

Command Syntax

- From the "**>**" prompt, use the following format,

ping <*ip-address*> [**interface** <*interface-name*>] [**packets** <*packets*>] [**vrf** <**mgmt-vrf** | *vrf-name*>] [**source** <*source-ip-address*>] [**deadline** <*deadline-time*>] [**ttl** <*ttl-value*>] [**interval** <*interval-value*>] [**pattern** <*pattern-value*>] [**size** <*size-value*>] [**tos** <*tos-value*>]

- From the "**#**" prompt, add **run** in front of the command,

run ping <*ip-address*> [**interface** <*interface-name*>] [**packets** <*packets*>] [**vrf** <**mgmt-vrf** | *vrf-name*>] [**source** <*source-ip-address*>] [**deadline** <*deadline-time*>] [**ttl** <*ttl-value*>] [**interval** <*interval-value*>] [**pattern** <*pattern-value*>] [**size** <*size-value*>] [**tos** <*tos-value*>]

Parameter

Parameter	Description
<*ip-address*>	Specifies the domain name or IPv4/IPv6 address of the destination host.
interface <*interface-name*>	Optional. Specifies the outgoing interface which can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
packets<*packets*>	Optional. Specifies the number of ICMP Echo Request packets sent.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be mgmt-vrf or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.
source <*source-ip-address*>	Optional. Specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.
deadline <*deadline-time*>	Optional. Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received. In this case ping does not stop after count packet are sent, it waits either for deadline to expire or until count probes are answered or for some error notification from network.
ttl <*ttl-value*>	Optional. Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 device that the message reaches sends an ICMP timeout message to the source host, indicating that the destination host is unreachable. The value is an integer that ranges from 1 to 255.
interval <*interval-value*>	Optional. Specify the interval for sending ICMP Echo Request message. The value is an integer in second.
pattern <*pattern-value*>	Optional. Specifies pad characters for ICMP Echo Request messages. By configuring pad characters for ICMP Echo Request messages, you can identify a specific message among the large number of received ICMP Echo Reply messages. The value is a hexadecimal integer.
size <*size-value*>	Optional. Specifies the maximum payload length of an ICMP Echo Request message. The value is an integer.
tos <*tos-value*>	Optional. Specifies the ToS value of the sent ICMP Echo Request messages. The ToS value is used to set the packet priority. The value is an integer that ranges from 0 to 254.

Example

- Check whether the host at 10.10.51.1 is reachable.

```
admin@Xorplus> ping 10.10.51.1
PING 10.10.51.1 (10.10.51.1) 56(84) bytes of data.
64 bytes from 10.10.51.1: icmp_seq=1 ttl=64 time=1.94 ms
64 bytes from 10.10.51.1: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 10.10.51.1: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 10.10.51.1: icmp_seq=4 ttl=64 time=146 ms
64 bytes from 10.10.51.1: icmp_seq=5 ttl=64 time=2.01 ms


--- 10.10.51.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.943/30.832/146.173/57.670 ms
```

traceroute

The **traceroute** command is used to check the route of packets when travelling from the source to the destination. When the network fails, the user can use this command to troubleshooting the fault point.

Command Syntax

- From the "**>**" prompt, use the following format,

traceroute <*ip-address*> [**vrf** <**mgmt-vrf** | *vrf-name*>]

- From the "**#**" prompt, add **run** in front of the command,

run traceroute <*ip-address*> [**vrf** <**mgmt-vrf** | *vrf-name*>]

Parameter

Parameter	Description
<*ip-address*>	Specifies the domain name or IPv4/IPv6 address of the destination host.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Traceroute the gateways for the host with the IP address 10.10.50.11.

```
admin@Xorplus> traceroute 10.10.50.11
traceroute to 10.10.50.11 (10.10.50.11), 30 hops max, 60 byte packets
 1  bogon (10.10.51.1)  3.063 ms  3.214 ms  3.370 ms
 2  bogon (10.10.50.11)  0.195 ms  0.172 ms  0.201 ms
```

- Traceroute the gateways for the host with the IP address fc00::3.

```
admin@Xorplus> traceroute fc00::3
traceroute to fc00::3 (fc00::3), 30 hops max, 60 byte packets
 1  bogon (FC00:1::3)  15 ms  20 ms  30 ms
 2  bogon (FC00::3)  1901 ms  1207 ms  3020 ms
```

tftp

The **tftp** command is used to transfer files between the local device and the TFTP server by TFTP protocol.

Command Syntax

- **Download a file:**
  - From the ">" prompt, use the following format,

    file tftp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

  - From the "**#**" prompt, add **run** in front of the command,

    run file tftp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

- **Upload a file:**
  - From the ">" prompt, use the following format,

    file tftp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

  - From the "**#**" prompt, add **run** in front of the command,

    run file tftp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

Parameter

Parameter	Description
get	Download a file.
put	Upload a file.
remote-file <*remote-file-path*>	Specifies the file path on TFTP server. The value is a string.
local-file <*local-file-path*>	Specifies the file path on local device. The value is a string.
ip-address <*ip-address*>	Specifies the IPv4/IPv6 address or host name for the TFTP server. The value is a string.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Usage Guidelines

Use the TFTP service to upload or download files with the following precautions:

- Usually, the TFTP server specifies a directory as the **default TFTP directory**, when use the **tftp get remote-file** <*remote-file-path*> command, don't need give the full path for the file, just type the sub-directory of the default directory.

For example, suppose there is a file **fileA** in the default TFTP directory, we can run the following command to download this file:

```
Admin@Xorplus# run file tftp get remote-file fileA
```

- On the PICA8 switch, the TFTP downloaded file is saved in directory **/cftmp/** by default.

Example

- Download file syslog.txt from the root directory of the TFTP server to the local device. The IP address of the TFTP server is 10.1.1.1. Save the downloaded file to the local device as file syslog.bak.

```
admin@Xorplus> file tftp get remote-file syslog.txt local-file syslog.bak ip-address 10.1.1.1
```

set protocols sflow collector vrf mgmt-vrf

The **set protocols sflow collector vrf mgmt-vrf** command configures to run the sFlow service in management VRF.

Command Syntax

set protocols sflow collector <*ip-address*> **vrf mgmt-vrf**

Parameter

Parameter	Description
collector <*ip-address*>	Specifies an IP address of the sFlow collector. The value is an IPv4/IPv6 address.

Usage Guidelines

SFlow service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding collector is required to be route reachable in the VRF running sFlow service.

Note: The latest configuration overrides the previous one.

Example

- Configure the sFlow service to run in the management VRF.

```
admin@Xorplus# set protocols sflow collector 10.10.10.1 vrf mgmt-vrf
admin@Xorplus# commit
```

scp

The **scp** command is used to transfer files between the local device and the SCP server.

Command Syntax

- **Download a file:**
  - From the ">" prompt, use the following format,

    file scp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "**#**" prompt, add **run** in front of the command,

    run file scp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
- **Upload a file:**
  - From the ">" prompt, use the following format,

    file scp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "**#**" prompt, add **run** in front of the command,

    run file scp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

Parameter

Parameter	Description
get	Download a file.
put	Upload a file.
remote-file <*remote-file-path*>	Specifies the file path on SCP server. The value is a string.
local-file <*local-file-path*>	Optional. Specifies the file path on local device. The value is a string.
ip-address <*ip-address*>:<*port*>	Specifies the IPv4/IPv6 address and port for the SCP server. The value is a string.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Usage Guidelines

Use the SCP service to upload or download files with the following precautions:

- Usually, the SCP server specifies a directory as the **default SCP directory**, when using the **scp get remote-file** <*remote-file-path*> command, don't need give the full path for the file, just type the subdirectory of the default directory.

  For example, suppose there is a file **fileA** in the default SCP directory, we can run the following command to download this file:

```
admin@Xorplus> file scp get remote-file fileA
```

- On the Pica8 switch, the SCP downloaded file is saved in directory /**cftmp/** by default.

Example

- Download file syslog.txt from the root directory of the SCP server to the local device. The IP address of the SCP server is 10.1.1.1. Save the downloaded file to the local device as file syslog.bak.

```
admin@Xorplus> file scp get remote-file syslog.txt local-file syslog.bak ip-address 10.1.1.1
```

set system login banner

The **set system login banner** command configures the header information displayed on a terminal before login.

Command Syntax

set system login banner <*text*>

Parameter

Parameter	Description
banner <*text*>	Specifies the banner content. The value is a string. Configure the banner information you want to print in double quotes.

Example

- Configure a login banner before login.

```
admin@Xorplus# set system login banner "Welcome to system!"
```

upgrade2 image-file

The **upgrade2 image-file** command upgrades the system by using upgrade2 command from the CLI operational mode or configuration mode.

Command Syntax

upgrade2 image-file <*image-name*>

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

The default directory for image file is */cftmp* if users do not specify the file path.

Example

- Upgrade the system by using upgrade2 command.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin
```

upgrade2 image-file backup-file

The **upgrade2 image-file backup-file** command upgrades the system by using upgrade2 command from the CLI operational mode or configuration mode and saves the user files during the upgrade process.

Command Syntax

upgrade2 image-file <*image-name*> **backup-file** <*backup-file*>

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).
backup-file <*backup-file*>	Specify a user defined backup list (*.lst).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

During the upgrade process, the switch can automatically back up the following files in the following directories from the previous PICOS system:

```
/etc/passwd
/etc/shadow
/etc/group
/etc/gshadow
/etc/resolv.conf
./etc/network/interfaces
/etc/picos/picos_start.conf
/etc/picos/switch-public.key
/etc/picos/pica.lic
/pica/config/pica_startup.boot
/pica/config/pica.conf.01
/pica/config/pica.conf.02
/pica/config/pica.conf.03
/pica/config/pica.conf.04
/pica/config/pica.conf.05
/ovs/ovs-vswitchd.conf.db
/ovs/function.conf.db
/ovs/config/meters
/ovs/config/groups
/ovs/config/flows
/ovs/var/lib/openvswitch/pki/
/var/log/report_diag.log
/var/log/report_diag.log.1
/var/log/report_diag.log.2
/var/log/report_diag.log.3
/var/log/report_diag.log.4
/var/log/report_diag.log.5
/cftmp/upgrade.log
/cftmp/upgrade2.log
/cftmp/auto/
```

If you want to save user files that are not in the above default backup file list, you need to first create or specify a **.lst** file and then add all those files that need to be backed up to this **.lst** file. You can use the **backup-file=(*.lst)** option to achieve this, where (*.lst) is the user created file with **.lst** format or specify the file path to this file.

The default directories for image file and backup file are */cftmp* if users do not specify the file path.

For example:

```
admin@XorPlus> sudo upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin backup-file /admin/back_files.ls
```

In this example, **back_files.lst** is a user created file. The user has already added the file to back_files.lst that needs to be saved in the event of power off.

Example

- Upgrade the system by using upgrade2 command and save the user files during the upgrade process.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin backup-file /admin/back_files.lst
```

upgrade2 image-file factory-default

The **upgrade2 image-file factory-default** command upgrades the system by using upgrade2 command and recoveries configuration to factory default settings.

Command Syntax

upgrade2 image-file <*image-name*> **factory-default**

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

Example

- Upgrade the system by using upgrade2 command and recovery configuration to factory default settings.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin factory-default
```

upgrade2 image-file use-prev-config

The **upgrade2 image-file use-prev-config** command upgrades the system by using upgrade2 command, skip the un-compatible configuration and continue loading the remaining configuration after system starts up from the reboot.

Command Syntax

upgrade2 image-file <*image-name*> **use-prev-config**

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

The main function of **use-prev-config** option is to decide whether to load the previous configuration file after a system reboot when performing upgrade2 or rollback to another version. If there is a command line in the old version configuration file that is not supported in the new system, with **use-prev-config** option that command will be skipped and continue loading the remaining configuration.

By default, upgrade2 or rollback is performed without **use-prev-config** option.

The following table describes the usage of **use-prev-config** option when performing upgrade2 or rollback.

	upgrade2 (From old version to new version)	**rollback** (From current version to old version)
with use-prev-config	1. Load the configuration file of old version after system reboot. 2. If there is a command line in the old version configuration file that is not supported in the new system, skip it and continue loading the remaining configuration.	1. Load the configuration file of current version after system reboot. 2. If there is a command line in the current configuration file that is not supported in the old system, skip it and continue loading the remaining configuration.
without use-prev-config	1. Load the configuration file of old version after reboot. 2. If there is a command in the old version configuration file that is not supported in the new system, load default configuration file.	Load the old version configuration file after rebooting.

Example

- Upgrade the system by using upgrade2 command, skip the un-compatible configuration and continue loading the remaining configuration after system starts up from the reboot.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin use-prev-config
```

set system dns-server-ip

The **set system dns-server-ip** command configures an IP address for a DNS server.

Command Syntax

set system dns-server-ip <*dns-server-ip*>

Parameter

Parameter	Description
dns-server-ip <*dns-server-ip*>	Specifies the IP address of a DNS server. The value could be an IPv4 address or an IPv6 address.

Usage Guidelines

During dynamic domain name resolution, the device can send a query packet to the DNS server, requesting for the query result.

Example

- Configure a DNS server with the IP addresses 172.16.1.1.

```
admin@Xorplus# set system dns-server-ip 172.16.1.1
```

set system console idle-timeout

The **set system console idle-timeout** command configures the timeout duration for disconnection from a console connection.

Command Syntax

set system console idle-timeout *<idle-timeout>*

Parameter

Parameter	Description
idle-timeout *<idle-timeout>*	Specifies the timeout duration for disconnection from a console connection. The value is an integer that ranges from 0 to 2000000, in second. The default value is 0, indicating that the console connection remains alive until you close it.

Usage Guidelines

If a user logs in to the device and does not perform an operation from the console port, the user interface is occupied unnecessarily. You can run the **set system console idle-timeout** command to disconnect the user's terminal from the device after the timeout duration.

NOTE:

Configuration changes takes effect immediately after successfully commit.

Example

- Configure the timeout duration for disconnection from a console connection to 1800 seconds.

```
admin@Xorplus# set system console idle-timeout 1800
admin@Xorplus# commit
```

set system login multiline-banner message

The **set system login multiline-banner message** command configures the header information displayed on a terminal before login, this command can be used for printing multi-line informations.

Command Syntax

set system login multiline-banner <*line-number*> **message** <*text*>

Parameter

Parameter	Description
multiline-banner <*line-number*>	Specifies the line number. The value is an integer that ranges from 1 to 20.
message <*text*>	Specifies the banner content. The value is a string. Configure the banner information you want to print in double quotes.

Example

- Configure a multi-line login banner.

```
admin@Xorplus# set system login multiline-banner 1 message "**********NOTICE**********"
admin@Xorplus# set system login multiline-banner 2 message "This is a property of Pica8."
admin@Xorplus# set system login multiline-banner 3 message "All users log-in are subject to company monitoring!"
admin@Xorplus# set system login multiline-banner 4 message "**********"
admin@Xorplus# commit
```

set system login multiline-announcement message

The **set system login multiline-announcement message** command configures the announcement message displayed on a terminal after users login, this command can be used for printing multi-line informations.

Command Syntax

set system login multiline-announcement <*line-number*> **message** <*text*>

Parameter

Parameter	Description
multiline-announcement <*line-number*>	Specifies the line number. The value is an integer that ranges from 1 to 20.
message <*text*>	Specifies the announcement message. The value is a string. **NOTE:** Configure the announcement message you want to print in double quotes.

Example

- Configure a multi-line login announcement message.

```
admin@XorPlus# set system login multiline-announcement 1 message "*********************************************"
admin@XorPlus# set system login multiline-announcement 2 message "Welcome to the system!"
admin@XorPlus# set system login multiline-announcement 3 message "*********************************************"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

set system aaa radius source-interface

The **set system aaa radius source-interface** command sets the source interface the switch uses to connect to the RADIUS server.

Command Syntax

set system aaa radius source-interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the source interface. The value could be an L3 VLAN interface, loopback interface, routed interface or sub-interface that enabled inband management or eth0. By default, the source interface is eth0.

Usage Guidelines

NOTE:

- When using a L3 VLAN interface, loopback interface, routed interface or sub-interface as a source interface connecting to the RADIUS server, you have to enable inband management function by using commands **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.
- Remember to specify an IP address for the source interface.

Example

- Set the source interface the switch uses to connect to the RADIUS server to loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.1.1.1 prefix-length 32
admin@Xorplus# set system aaa radius source-interface loopback
```

- Set the source interface the switch uses to connect to the RADIUS server to L3 VLAN interface.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 100
admin@Xorplus# set l3-interface vlan-interface vlan100 address 10.10.51.129 prefix-length 24
admin@Xorplus# set vlans vlan-id 100 l3-interface vlan100
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# set system aaa radius source-interface vlan100
```

set protocols grpc enable

The **set protocols grpc enable** command e**nables** gRPC agent on the device, which supports the gNMI interface for dial-in mode of Telemetry technology.

The **delete protocols grpc enable** command disables the gRPC agent function on the device.

Command Syntax

set protocols grpc enable <**true | false**>

Parameter

Parameter	Description
enable <true | false>	Enables or disables gRPC agent function on the device**.** The value could be **true** or **false**. • **true**: Enables gRPC agent function**.** • **false**: Disables gRPC agent function. By default, gRPC agent function is disabled.

Example

- Enable gRPC agent.

```
admin@Xorplus# set protocols grpc enable true
admin@Xorplus# commit
```

set protocols grpc port

The **set protocols grpc port** command configures the listening port number for the gRPC agent.

Command Syntax

set protocols grpc port <*port-number*>

Parameter

Parameter	Description
port <*port-number*>	Specifies the listening port number for the gRPC agent. The value is an integer that ranges from 1024 to 65535. The default value is 9339.

Example

- Configure the listening port number for the gRPC agent.

```
admin@Xorplus# set protocols grpc port 10500
admin@Xorplus# commit
```

set system ztp enable

The **set system ztp enable** command can be used to enable or disable ZTP (Zero Touch Provisioning) function.

Command Syntax
set system ztp enable <true | false>

Parameter

Parameter	Description
enable <true | false>	Configures whether to enable or disable the ZTP function. The value is **true** or **false**. **true**: enables the ZTP function. **false**: disables the ZTP function. The default value is **true**.

Usage Guidelines

By default, the ZTP function is enabled, and the ZTP process is automatically performed when the device boots up with empty configuration. Users can disable ZTP function if they do not want the device to perform ZTP process when booting with empty configuration.

Example

• Disable the ZTP function.

```
admin@XorPlus# set system ztp enable false
admin@XorPlus# commit
```

telnet

The **telnet** command is used to connect to remote servers from the current device using the Telnet protocol. Before using the telnet command to connect to a Telnet server, the Telnet client and the Telnet server need to be route reachable, and the Telnet service must be enabled on the Telnet server side.

Command Syntax

- From the "**>**" prompt, use the following format,

telnet {<*ip-address*>|<*host-name*>} [<*port-number*>] [**vrf** <*vrf-name*>]

- From the "**#**" prompt, add **run** in front of the command,

run telnet {<*ip-address*>|<*host-name*>} [<*port-number*>] [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
<*ip-address*>|<*host-name*>	Specifies the IPv4/IPv6 address or host name of a remote system.
<*port-number*>	Optional. Specifies the TCP port number on which the remote device provides Telnet service. The value is an integer that ranges from 1 to 65535. The default value is 23.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Establish a Telnet connection with a remote device in default VRF.

```
admin@PICOS>  telnet 10.10.51.205 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

- Establish a Telnet connection with a remote device in management VRF.

```
admin@PICOS>  telnet 10.10.51.25 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

set system start-shell-sh password

The **set system start-shell-sh password** command configures the password when using command ***run start shell sh*** to entering Linux shell.

The **delete system start-shell-sh password** command deletes the configuration.

Command Syntax

set system start-shell-sh password <*password*>

delete system start-shell-sh password

Parameter

Parameter	Description
password <*password*>	Specifies the password for entering Linux shell. The value is a string, spaces are not allowed, case-sensitive, and can be 6 to 48 characters long. By default, there is no password for entering Linux shell.

Usage Guidelines

The configuration takes effect immediately after successfully commit.

When showing the configuration, the password is displayed as ciphertext.

Example

- Configure the password for entering Linux shell and enter Linux shell with this password.

```
admin@PICOS# set system start-shell-sh password 123456abc
admin@PICOS# commit
admin@PICOS# run start shell sh 123456abc
admin@PICOS:~$
```

set system services telnet disable

The **set system services telnet disable** command can be used to enable or disable the telnet service function. The Pica8 switch supports functioning as a telnet server. To enable the telnet server function, users can enable the telnet service by using this command.

The **delete system services telnet disable** command deletes the configuration.

NOTEs:

- Users need to enable telnet service to enable telnet server function on the device.
- Telnet service is insecure. Do not enable a telnet server if you don't know what exactly it may mean.
- Limit to a maximum of 20 connections within 10 seconds.
- Terminate the session in 60 seconds if the connection is not successful.

Command Syntax

set system services telnet disable <**true | false**>

delete system services telnet disable

Parameter

Parameter	Description
enable <**true	false**>	Enable or disable telnet service. The value could be **true** or **false**. • **true**: Enable telnet service. • **false**: Disable telnet service. By default, telnet service is disabled.

Example

- Enable telnet service.

```
admin@PICOS# set system services telnet disable false
admin@PICOS# commit
```

set system services web disable

The **set system services web disable** command is used to enable or disable the web service on the system, which typically prevents access to the device's web-based management interface. This enhances security by reducing potential attack surfaces, especially if the web interface is not in use or required.

The **delete system services web disable** command deletes the configuration.

Command Syntax

set system services web disable <**true | false**>

delete system services web disable

Parameters

Parameter	Description
disable <true | false>	Enables or disables the web service on the system. The value is **true** or **false**. • **true**: disables the web service on the system. • **false**: enables the web service on the system.

Usage Guidelines

Not all devices support this command; only platforms that support the PICOS web configuration interface can apply this configuration. For specific compatibility details, please refer to PICOS-WEB_User_Configuration_Manual .

Among the platforms supporting the PICOS web configuration interface, the default settings for web access may vary:

- **ARM models**: Web access is enabled by default.
- **X86 models**: Web access is disabled by default.

The device model (ARM or X86) can be identified using the Linux command:

```
admin@PICOS:~$ uname -m
armv7l
admin@leaf04:~$ uname -m
x86_64
```

Example

- Enable web service on the system.

```
admin@PICOS# set system services web disable false
admin@PICOS# commit
```

Interface Configuration Commands

This section contains descriptions of the CLI commands that this chapter references.

- interface aggregate-balancing hash-mapping field ethernet-destination-address disable
- interface aggregate-balancing hash-mapping field ethernet-source-address disable
- interface aggregate-balancing hash-mapping field ethernet-type disable
- interface aggregate-balancing hash-mapping field ingress-interface disable
- interface aggregate-balancing hash-mapping field ip-destination disable
- interface aggregate-balancing hash-mapping field ip-protocol disable
- interface aggregate-balancing hash-mapping field ip-source disable
- interface aggregate-balancing hash-mapping field port-destination disable
- interface aggregate-balancing hash-mapping field port-source disable
- interface aggregate-balancing hash-mapping field vlan disable
- interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control
- interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port
- interface aggregate-ethernet <lag_name> backup-port delay
- interface aggregate-ethernet <lag_name> backup-port interface
- interface aggregate-ethernet <lag_name> backup-port mode
- interface aggregate-ethernet <lag_name> crossflow enable
- interface aggregate-ethernet <lag_name> crossflow local-control
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode
- interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id
- interface aggregate-ethernet <lag_name> hash-mapping mode
- interface aggregate-ethernet <lag_name> mtu
- interface aggregate-ethernet <lag_name> snmp-trap
- interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan
- interface aggregate-ethernet <lag_name> storm-control <mode> pps
- interface cut-through-mode
- interface ecmp max-path
- interface ethernet-switching-options buffer queue-limit
- interface ethernet-switching-options mac-table-aging-time
- interface gigabit-ethernet <port> backup-port delay
- interface gigabit-ethernet <port> backup-port interface
- interface gigabit-ethernet <port> backup-port mode
- interface gigabit-ethernet <port> crossflow enable
- interface gigabit-ethernet <port> crossflow local-control
- interface gigabit-ethernet <port> description
- interface gigabit-ethernet <port> disable
- interface gigabit-ethernet <port> ether-options flow-control
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode
- interface gigabit-ethernet <port> family ethernet-switching native-vlan-id
- interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged
- interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>
- interface gigabit-ethernet <port> mac-learning <boolean>
- interface gigabit-ethernet <port> mtu
- interface gigabit-ethernet <port> power-preemphasis-level
- interface gigabit-ethernet <port> snmp-trap
- interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>
- interface gigabit-ethernet <port> storm-control <mode> kbps
- interface gigabit-ethernet <port> storm-control <mode> pps
- interface gigabit-ethernet <port> storm-control <mode> ratio <value>
- interface gigabit-ethernet <port> wred queue <value> drop_probability
- interface gigabit-ethernet <port> wred queue <value> ecn_thresh
- interface gigabit-ethernet <port> wred queue <value> enable
- interface gigabit-ethernet <port> wred queue <value> max_thresh
- interface gigabit-ethernet <port> wred queue <value> min_thresh
- interface max-acl-rule-limit <egress/ingress>
- interface max-route-limit

- IPv6 Neighbor Discovery Protocol Command Reference
  - set l3-interface routed-interface ipv6-nd adv-interval-option
  - set l3-interface routed-interface ipv6-nd home-agent-config-flag
  - set l3-interface routed-interface ipv6-nd home-agent-lifetime
  - set l3-interface routed-interface ipv6-nd home-agent-preference
  - set l3-interface routed-interface ipv6-nd managed-config-flag
  - set l3-interface routed-interface ipv6-nd mtu
  - set l3-interface routed-interface ipv6-nd other-config-flag
  - set l3-interface routed-interface ipv6-nd prefix off-link
  - set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
  - set l3-interface routed-interface ipv6-nd prefix router-address
  - set l3-interface routed-interface ipv6-nd prefix valid-lifetime
  - set l3-interface routed-interface ipv6-nd ra-fast-retrans
  - set l3-interface routed-interface ipv6-nd ra-interval
  - set l3-interface routed-interface ipv6-nd ra-lifetime
  - set l3-interface routed-interface ipv6-nd reachable-time
  - set l3-interface routed-interface ipv6-nd router-preference
  - set l3-interface routed-interface ipv6-nd suppress-ra
  - set l3-interface vlan-interface ipv6-nd adv-interval-option
  - set l3-interface vlan-interface ipv6-nd home-agent-config-flag
  - set l3-interface vlan-interface ipv6-nd home-agent-lifetime
  - set l3-interface vlan-interface ipv6-nd home-agent-preference
  - set l3-interface vlan-interface ipv6-nd managed-config-flag
  - set l3-interface vlan-interface ipv6-nd mtu
  - set l3-interface vlan-interface ipv6-nd other-config-flag
  - set l3-interface vlan-interface ipv6-nd prefix off-link
  - set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
  - set l3-interface vlan-interface ipv6-nd prefix router-address
  - set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
  - set l3-interface vlan-interface ipv6-nd ra-fast-retrans
  - set l3-interface vlan-interface ipv6-nd ra-interval
  - set l3-interface vlan-interface ipv6-nd ra-lifetime
  - set l3-interface vlan-interface ipv6-nd reachable-time
  - set l3-interface vlan-interface ipv6-nd router-preference
  - set l3-interface vlan-interface ipv6-nd suppress-ra
- L3 Interface
  - run clear l3-interface statistics
  - run show l3-interface
  - run show l3-interface loopback
  - run show l3-interface routed-interface
  - run show l3-interface vlan-interface
  - set l3-interface loopback address
  - set l3-interface loopback disable
  - set l3-interface loopback vrf
  - set l3-interface routed-interface address
  - set l3-interface routed-interface description
  - set l3-interface routed-interface dhcp
  - set l3-interface routed-interface mtu
  - set l3-interface routed-interface pmtu-discovery
  - set l3-interface routed-interface rate-limit
  - set l3-interface routed-interface vrf
  - set l3-interface vlan-interface address prefix-length
  - set l3-interface vlan-interface dhcp
  - set l3-interface vlan-interface mtu
  - set l3-interface vlan-interface pmtu-discovery
  - set l3-interface vlan-interface rate-limit
  - set l3-interface vlan-interface vrf
- Port Security Commands
  - run clear port-security dynamic address
  - run clear port-security dynamic interface
  - run clear port-security port-error
  - run clear port-security sticky address
  - run clear port-security sticky interface
  - run show port-security address
  - run show port-security brief
  - run show port-security interface
  - set interface ethernet-switching-options port-error-discard timeout
  - set interface gigabit-ethernet port-security block
  - set interface gigabit-ethernet port-security mac-address vlan
  - set interface gigabit-ethernet port-security mac-limit
  - set interface gigabit-ethernet port-security sticky

    - set interface gigabit-ethernet port-security violation
- Routed Interface
    - run show interface routed-interface brief
    - run show vlans routed-vlan
    - set interface aggregate-ethernet routed-interface enable
    - set interface aggregate-ethernet routed-interface name
    - set interface aggregate-ethernet routed-interface sub-interface vlan-id
    - set interface gigabit-ethernet routed-interface enable
    - set interface gigabit-ethernet routed-interface name
    - set interface gigabit-ethernet routed-interface sub-interface
    - set vlans reserved-vlan
- run show interface diagnostics tdr
- run show interface port-index-mapping
- set interface aggregate-ethernet
- set interface aggregate-ethernet aggregated-ether-options lacp
- set interface aggregate-ethernet aggregated-ether-options lacp fallback enable
- set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout
- set interface aggregate-ethernet description
- set interface aggregate-ethernet disable
- set interface aggregate-ethernet family ethernet-switching port-mode
- set interface aggregate-ethernet family ethernet-switching vlan members
- set interface bpdu-tunneling destination-mac
- set interface ecmp hash-mapping dlb-assigned
- set interface ecmp hash-mapping dlb-normal
- set interface ecmp hash-mapping dlb-optimal
- set interface ecmp hash-mapping field ingress-interface disable
- set interface ecmp hash-mapping field ip-destination disable
- set interface ecmp hash-mapping field ip-protocol disable
- set interface ecmp hash-mapping field ip-source disable
- set interface ecmp hash-mapping field port-destination disable
- set interface ecmp hash-mapping field port-source disable
- set interface ecmp hash-mapping field vlan disable
- set interface ecmp hash-mapping randomized-load-balancing
- set interface ecmp hash-mapping resilient-load-balancing
- set interface ecmp hash-mapping round-robin-load-balancing
- set interface ecmp hash-mapping symmetric
- set interface gigabit-ethernet auto-speeds
- set interface gigabit-ethernet breakout
- set interface gigabit-ethernet breakout-type
- set interface gigabit-ethernet cdr
- set interface gigabit-ethernet duplex auto
- set interface gigabit-ethernet ether-options 802.3ad
- set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol
- set interface gigabit-ethernet family ethernet-switching port-mode
- set interface gigabit-ethernet family ethernet-switching vlan members
- set interface gigabit-ethernet fec
- set interface gigabit-ethernet speed
- set interface gigabit-ethernet up-mode
- set management-ethernet-speed eth0
- show interface aggregate-ethernet <lag_name>
- show interface aggregate-ethernet <lag_name> dot1q-tunneling
- show interface bpdu-tunneling
- show interface brief
- show interface detail
- show interface diagnostics optics all
- show interface ecmp max-path
- show interface flexlink
- show interface gigabit-ethernet <interface>
- Uplink Failure Detection Commands
    - run show interface ufd
    - set interface ufd link-to-disable
    - set interface ufd link-to-monitor

Port Security Commands

- set interface gigabit-ethernet port-security mac-address vlan
- set interface gigabit-ethernet port-security mac-limit
- set interface gigabit-ethernet port-security sticky
- set interface gigabit-ethernet port-security violation
- set interface gigabit-ethernet port-security block
- set interface ethernet-switching-options port-error-discard timeout
- run show port-security brief
- run show port-security address
- run show port-security interface
- run clear port-security port-error
- run clear port-security sticky interface
- run clear port-security sticky address
- run clear port-security dynamic interface
- run clear port-security dynamic address

set interface gigabit-ethernet port-security mac-address vlan

The **set interface gigabit-ethernet port-security mac-address vlan** command configures a static secure MAC address.

The **delete interface gigabit-ethernet port-security mac-address vlan** command removes a static secure MAC address. No clear command can be used to remove a static secure MAC address.

Command Syntax
set interface gigabit-ethernet <*interface-name*>**port-security mac-address** <*mac-addr*> **vlan**<*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
mac-address <*mac-addr*>	Specifies a static secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. Note that, the MAC address cannot be configured to a multicast MAC or the system MAC.
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

After port security is enabled, the dynamic MAC addresses learned on the secure interface will be changed to dynamic secure MAC addresses. When the secure interface goes down and up, or device reboots or restarts, dynamic secure MAC addresses are lost and need to be re-learned.

Dynamic secure MAC addresses will be aged out by the MAC aging time.

However, static secure MAC table entries are not lost in the case of interface state changing to down or the switch restarted or rebooted. The command **set interface gigabit-ethernet** <*port-name*> **port-security mac-address** <*mac-addr*> **vlan** <*vlan-id*> can be used to configure the

static secure MAC address.

NOTE:

- Static secure MAC addresses have a higher priority than dynamic secure MAC addresses.
- Once a MAC address is bound to a port, it's not allowed to bind this MAC to another port.

Example

- Configure a static secure MAC address.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 port-security mac-address 22:00:00:00:00:00 vlan 1
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security mac-limit

The **set interface gigabit-ethernet port-security mac-limit** command configures the maximum number of secure MAC addresses that can be learned on an interface.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security mac-limit** <*mac-limit*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
mac-limit <*mac-limit*>	Specifies the maximum number of secure MAC addresses that can be learned by an interface. The value is an integer that ranges from 1 to 1024. The default value is 1.

Usage Guidelines

The MAC limit number is used to limit the number of secure MAC of the interface, including the number of dynamic secure MAC and manually configured static secure MAC. If sticky is enabled, MAC limit includes sticky secure MAC and static secure MAC.

A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.

If you are trying to configure a static secure MAC address and it exceeds the MAC limit, your configuration is rejected and an error message is displayed. If it reaches the MAC limit and a new dynamic secure MAC address is learned, a violation action is triggered. For details about violation, please see set interface gigabit-ethernet port-security violation.

NOTE:

When setting a MAC limit value for a secure interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of the secure addresses on the interface exceeds the new value, the command is rejected. In this case, you can remove the secure addresses to the number less than the new MAC limit value.

Example

- Configure the maximum number of secure MAC addresses that can be learned on an interface.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-limit 10
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security sticky

The **set interface gigabit-ethernet port-security sticky** command is used to enable or disable the sticky function on an interface.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security sticky** <**true** | **false**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
sticky <true | false>	Enables or disables the sticky function on an interface. The value could be **true** or **false**. • **true**: enables the sticky MAC function • **false**: disables the sticky MAC function. By default, sticky function is disabled.

Usage Guidelines

When the secure port goes down and up, dynamic secure MAC addresses will be cleared by the system. You can enable the sticky function to solve this problem.

After enabled the sticky function, the dynamic secure MAC addresses learned on the port are converted to sticky secure MAC. The sticky MAC will not be aged, and the sticky MAC table entries will not be lost when the port is down and up.

NOTE:

- When the switch reboots or restarts, sticky secure MAC addresses are lost and need to be re-learned.
- Disabling the sticky function converts the sticky secure MAC addresses on the current interface to dynamic secure MAC addresses.

Example
• Enable the sticky function on interface ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security sticky true
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security violation

The **set interface gigabit-ethernet port-security violation** command configures a protective action for the system to perform when the number of learned MAC addresses exceeds the MAC limit.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security violation** <**protect | restrict | shutdown | shutdown-temp**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
violation <**protect** | **restrict** | **shutdown** | **shutdown-temp**>	Specifies the protective action. The value could be **protect**, **restrict**, **shutdown** or **shutdown-temp**. • **protect**: Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit. • **restrict**: Discards packets with new source MAC addresses and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. • **shutdown**: Shuts the interface down, sets the interface status to error-disabled and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. User can recover the port with the **run clear port-security port-error** command. • **shutdown-temp**: Shuts the interface down temporarily, sets the interface status to error-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. After 20 seconds (default), the interface comes up. The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is configured to **shutdown-temp**. The default value is **protect**.

Usage Guidelines

If it reaches the MAC limit and you are trying to configure a static secure MAC address, your configuration is rejected and an error message is displayed. If it reaches the MAC limit and a new dynamic secure MAC address is added, a violation action is triggered.

Example
• Configure the protective action for the system to perform when the number of learned MAC addresses exceeds the limit to **shutdown**.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security violation shutdown
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security block

The **set interface gigabit-ethernet port-security block** command configures the type of packets that will be blocked in the egress direction of the secure port.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **port-security block** <**all | broadcast | multicast | uni-multi-cast | unicast**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
block <**all** | **broadcast** | **multicast** | **uni-multi-cast** | **unicast**>	Specifies the packet type which will be blocked on the egress direction of the port enabled with port security. The value could be **all**, **broadcast**, **multicast**, **uni-multi-cast** or **unicast**. • **all**: Discards all the packets in egress direction of the port. • **broadcast**: Discards only the broadcast packets in egress direction of the port. • **multicast**: Discards only the multicast packets in egress direction of the port. • **uni-multi-cast**: Discards both the unknown unicast packets and multicast packets in egress direction of the port. • **unicast**: Discards only the unknown unicast packets in egress direction of the port. By default, packets will not be blocked by port security in egress direction of the port.

Example

• Configure to discard only the broadcast packets in egress direction of the port.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security block broadcast
admin@XorPlus# commit
```

set interface ethernet-switching-options port-error-discard timeout

The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is **shutdown-temp**.

Command Syntax
set interface ethernet-switching-options port-error-discard timeout <*seconds*>

Parameter

Parameter	Description
timeout <*seconds*>	Specifies the port recovery interval when the port security violation mode is **shutdown-temp**. The value is an integer, in seconds, that ranges from 10 to 300. The default value is 20 seconds.

Example
• Configure the port recovery interval when the port security violation mode is shutdown-temp.

```
admin@XorPlus# set interface ethernet-switching-options port-error-discard timeout 10
admin@XorPlus#commit
```

run show port-security brief

The **run show port-security brief** command briefly displays the port security configuration and statistics information for all the secure ports.

Command Syntax

run show port-security brief

Parameter

None.

Example

- Run the command **run show port-security brief** to briefly view the port security configuration and statistics information.

```
admin@Xorplus# run show port-security brief
Secure Port    MaxMacLimit    CurrentAddr    ViolationCount    Action
-------------------------------------------------------------------------------------------------------------------
ge-1/1/22      2              0              0                 restrict
ge-1/1/23      1              0              0                 shutdown-temp
ge-1/1/34      1              0              0                 protect
```

Table 1. Description of the run show port-security brief command output

Item	Description
Secure Port	Indicates the port enabled port security.
MaxMacLimit	Indicates the maximum number of secure MAC addresses that can be learned on the interface.
CurrentAddr	Indicates the secure MAC addresses on the interface.
ViolationCount	The number of times that violation was triggered. Note that port security violations are counted only if the port security violation mode is **restrict**, **shutdown**, or **shutdown-temp**.
Action	Indicates the protective action for the system to perform when the number of learned MAC addresses exceeds the limit. The value could be **protect**, **restrict**, **shutdown** or **shutdown-temp**.

run show port-security address

The **run show port-security address** command displays the secure MAC address table entries.

Command Syntax

run show port-security [**interface gigabit-ethernet** <*interface-name*>] **address**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies a secure interface name. The value is a string. • If no interface name is specified, the secure MAC address table entries of all the secure ports are displayed. • If an interface name is specified, only the secure MAC address table entries of the specific secure port are displayed.

Example

- Run **run show port-security address** command to view the secure MAC address table entries.

```
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ---------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:11:11:11:12 dynamic ge-1/1/1
1 00:00:23:23:23:23 static ge-1/1/1
1 00:00:23:23:23:24 static ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

- Run **run show port-security interface gigabit-ethernet** <*interface-name*> **address** command to view the secure MAC address table entries on a secure interface.

```
admin@Xorplus# run show port-security interface gigabit-ethernet ge-1/1/34 address
            Secure Mac Address Table
-----------------------------------------------------
VLAN  MAC Address      Type     Interface
----     -----------------      -------    ----------
1       00:00:11:11:11:11  dynamic   ge-1/1/1
-----------------------------------------------------
MAC age time    :300s
```

run show port-security interface

The **run show port-security interface** command displays the detailed port security configuration and statistical information based on secure ports.

Command Syntax

run show port-securityinterface [**gigabit-ethernet** <*interface-name*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies a secure interface name. The value is a string. • If no interface name is specified, the detailed port security configuration and statistical information of all the secure ports are displayed. • If an interface name is specified, only the detailed port security configuration and statistical information of the specific secure port are displayed.

Example

- Run **run show port-security interface** command to view the detailed port security configuration and statistical information of all the secure ports.

```
admin@Xorplus# run show port-security interface
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/23
---------------------------------------
Port Security               : enabled
Violation action            : shutdown-temp
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/34
---------------------------------------
Port Security               : enabled
Violation action            : protect
Block type                  : N/A
Sticky                      : false
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

- Run command **run show port-security interface gigabit-ethernet** <*interface-name*> to view the detailed port security configuration and statistical information of a specific secure port.

```
admin@Xorplus# run show port-security interface gigabit-ethernet ge-1/1/22
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
```

```
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

run clear port-security port-error

When the port security violation mode is **shutdown**, the port will be set to the *error-discard* state when detecting a violation. User can recover the port with the **run clear port-security port-error** command.

Command Syntax

run clear port-security port-error interface {**all | gigabit-ethernet** <*interface-name*>}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name.

Example

- Run the command **run clear port-security port-error** to recover the port ge-1/1/33.

```
admin@Xorplus# run clear port-security port-error interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security sticky interface

The **run clear port-security sticky interface** command clears the sticky secure MAC addresses of a secure interface.

Command Syntax

run clear port-security sticky interface {**all | gigabit-ethernet** <*interface-name*> [**vlan** <*vlan-id*>]}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name. The value could **all** or a specific interface name.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security sticky interface** to clear the sticky secure MAC addresses of ge-1/1/33.

```
admin@Xorplus# run clear port-security sticky interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security sticky address

The **run clear port-security sticky address** command clears a sticky secure MAC address.

Command Syntax

run clear port-security sticky address <*mac-addr*> [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
address <*mac-addr*>	Specifies a secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security sticky address** to clear a sticky secure MAC address.

```
admin@Xorplus# run clear port-security sticky address 00:00:0a:00:00:01
Clear done.
```

run clear port-security dynamic interface

The **run clear port-security dynamic interface** command clears the dynamic secure MAC addresses of a secure interface.

Command Syntax

run clear port-security dynamic interface {**all | gigabit-ethernet** <*interface-name*> [**vlan** <*vlan-id*>]}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name. The value could **all** or a specific interface name.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security dynamic interface** to clear the dynamic secure MAC addresses of ge-1/1/33.

```
admin@Xorplus# run clear port-security dynamic interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security dynamic address

The **run clear port-security dynamic address** command clears a dynamic secure MAC address.

Command Syntax

run clear port-security dynamic address <*mac-addr*> [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
address <*mac-addr*>	Specifies a secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security dynamic address** to clear a dynamic secure MAC address.

```
admin@Xorplus# run clear port-security dynamic address 00:00:0a:00:00:01
Clear done.
```

L3 Interface

- set l3-interface vlan-interface vrf
- set l3-interface vlan-interface address prefix-length
- set l3-interface loopback address
- set l3-interface loopback disable
- set l3-interface loopback vrf
- set l3-interface vlan-interface rate-limit
- set l3-interface vlan-interface mtu
- set l3-interface vlan-interface dhcp
- run show l3-interface vlan-interface
- run show l3-interface
- run show l3-interface loopback
- run clear l3-interface statistics
- set l3-interface routed-interface dhcp
- set l3-interface routed-interface rate-limit
- set l3-interface routed-interface mtu
- set l3-interface routed-interface vrf
- set l3-interface routed-interface address
- set l3-interface routed-interface description
- run show l3-interface routed-interface
- set l3-interface vlan-interface pmtu-discovery
- set l3-interface routed-interface pmtu-discovery

set l3-interface vlan-interface vrf

The **set l3-interface vlan-interface vrf** command is used to bind the Layer 3 VLAN interface to the VRF.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

By binding the Layer 3 VLAN interfaces to different VRFs, the system segregates the IP routing table, ARP table, hardware forwarding table and host hardware forwarding table of different VRFs in customer edge devices.

Note that: The Layer 3 VLAN interface is in the default VRF if not explicitly bound to any VRF.

Example

- Bind the Layer 3 VLAN interface VLAN10 to the VRF vrf1.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 vrf vrf1
admin@Xorplus# commit
```

set l3-interface vlan-interface address prefix-length

To configure an IPv4 or IPv6 address for an L3 interface, use the **set l3-interface vlan-interface address prefix-length** command in L2/L3 configuration mode. To remove an L3 interface, use the **delete** form of the command.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>
delete l3-interface vlan-interface <*interface-name*>

Parameters

Parameter	Description
vlan-interface <*interface-name*>	Interface name.
address	IPv4 or IPv6 address.
number	The network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Example

- The following example configures the IPv4 address for the *vlan10* L3 interface and then removes the L3 interface:

```
admin@Switch# set l3-interface vlan-interface vlan10 address 192.168.1.1 prefix-length 24
admin@Switch# commit
admin@Switch# delete l3-interface vlan-interface vlan10
```

- The following example configures the IPv6 address for the *vlan20* L3 interface and then removes the L3 interface:

```
admin@Switch# set l3-interface vlan-interface vlan20 address 2001:1:1::1 prefix-length 64
admin@Switch# commit
admin@Switch# delete l3-interface vlan-interface vlan20
```

set l3-interface loopback address

The **set l3-interface loopback address** command creates a loopback interface and configures its IP address.

Command Syntax

set l3-interface loopback <*loopback-name*> **address** <*ip-address*> **prefix-length** <*int*>

Parameters

Parameter	Description
loopback <*loopback-name*>	Specifies a loopback interface. The value is a string.
address <*ip-address*>	Specifies the IP address of a loopback interface. • Ipv4 default value: 127.0.0.1 • Ipv6 default value: ::1
prefix-length <*int*>	The IPv4 network prefix length is fixed to 32. The IPv6 network prefix length is fixed to 128.

Usage Guidelines

A loopback interface is always Up.

The IP address of a loopback interface is usually specified as the source address of packets.

After a loopback interface is created, you can use command **set l3-interface loopback vrf** to bind the loopback interface to a VRF. Users can configure multiple loopback interfaces per VRF. A loopback interface is in the default VRF by default.

You can also use command **set l3-interface loopback disable** to disable a loopback interface. When a loopback interface is created, it is enabled by default.

Note that **lo** is a built-in loopback interface in default VRF, it cannot be bound to any other user-defined VRF, or be disabled.

Example

- Create a loopback interface **lo-gre** in the default VRF.

```
admin@Xorplus# set l3-interface loopback lo-gre address 1.1.1.1 prefix-length 32
admin@Xorplus# commit
```

set l3-interface loopback disable

The **set l3-interface loopback disable** command can be used to enable or disable a loopback interface.

Command Syntax

set l3-interface loopback <*interface-name*> **disable** <**true | false**>

Parameters

Parameter	Description
loopback <*interface-name*>	Specifies the name of the loopback interface. The value is a string.
disable <**true	false**>	Enables or disables the loopback interface. The value could be **true** or **false**. • **true**: Disable the loopback interface. • **false**: Enable the loopback interface. When a loopback interface is created, it is enabled by default.

Example

- Disable loopback interface lo2.

```
admin@Xorplus# set l3-interface loopback lo2 disable true
admin@Xorplus# commit
```

set l3-interface loopback vrf

The **set l3-interface loopback vrf** command can be used to bind the loopback interface to a VRF. Multiple loopback interfaces can be configured within a user configured VRF or the default VRF.

Command Syntax

set l3-interface loopback <*interface-name*> **vrf** <*vrf-name*>

Parameters

Parameter	Description
loopback <*interface-name*>	Specifies the name of the loopback interface. The value is a string.
vrf <*vrf-name*>	Specifies the name of the VRF for the loopback interface.

Example

- Bind the loopback interface lo2 to vrf2.

```
admin@Xorplus# set l3-interface loopback lo2 vrf vrf2
admin@Xorplus# commit
```

set l3-interface vlan-interface rate-limit

The **set l3-interface vlan-interface rate-limit** command configures the CPU egress rate limit for an L3 VLAN interface.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **rate-limit** <*rate-limit*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
rate-limit <*rate-limit*>	Specifies an egress rate limit for the L3 VLAN interface. The value is an integer, in kbps, that ranges from 1 to 1000000000. By default, there is no rate limit for the L3 VLAN interface in the outbound direction.

Usage Guidelines

L3 VLAN interface rate limit is applied to packets delivered out from the CPU, controlling shock of large flow on CPU, releasing the burden on CPU.

Example

- Configure rate limit for the L3 VLAN interface vlan200.

```
admin@Xorplus# set l3-interface vlan-interface vlan200 rate-limit 1024
admin@Xorplus# commit
```

set l3-interface vlan-interface mtu

The **set l3-interface vlan-interface mtu** command configures the maximum transmission unit (MTU) of a Layer 3 VLAN interface.

> **NOTE:**
>
> The MTU value takes effect only on the outbound interface of the Layer 3 VLAN interface.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **mtu** <*mtu-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
mtu <*mtu-value*>	Specifies the MTU of an interface. The value is an integer that ranges from 68 to 65535, in bytes. The default value is 1500 bytes.

Usage Guidelines

An MTU value determines the maximum number of bytes in the IP layer packet that can be sent at a time. If the size of the data packets of the IP layer packet exceeds the MTU supported by a transit node or a receiver, the data packet is dropped at the sender's IP layer.

Example

- Configure the MTU of the VLAN interface vlan10 as 2000.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 mtu 2000
```

set l3-interface vlan-interface dhcp

DHCP can be enable or disable on this VLAN interface as dhcp client. The VLAN interface will get ip address by DHCP server if DHCP is enable on this VLAN interface.

Command Syntax
set l3-interface vlan-interface <*interface-name*> **dhcp** <*boolean*>

Parameter
•<*interface-name*> *Vlan interface name is defined*.
•<*boolean*> *enable or disable dhcp on vlan-interface as client*. The value include:

- **true** Enable DHCP client on this vlan interface.
- **False** Default configuration. Disable DHCP client on this VLAN interface.

Example

- This example manually enables DHCP on the VLAN interface.

```
admin@XorPlus#set l3-interface vlan-interface vlan2 dhcp true
admin@XorPlus# commit
```

run show l3-interface vlan-interface

To display information about an L3 VLAN interface, use the **run show l3-interface vlan-interface** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface vlan-interface <*interface-name*> [**detail**]

Parameters

Parameter	Description
interface-name	Optional. The VLAN interface name.
detail	Optional. Show detail informations of all VLAN interface.

Example

- The following example displays information about **vlan10**:

```
admin@Switch# run show l3-interface vlan-interface vlan10
vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.............................0
              IPv4 Forwarding Packets........................0
              IPv6 Input Packets.............................0
              IPv6 Forwarding Packets........................0
```

- The following example displays the detail information about **vlan10**:

```
admin@Switch# run show l3-interface vlan-interface vlan10 detail
vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.............................0
              IPv4 Forwarding Packets........................0
              IPv6 Input Packets.............................0
              IPv6 Forwarding Packets........................0
            Port        State         Tag
            ----------  ------------  --------
            te-1/1/1    FORWARDING    tagged
            te-1/1/17   DOWN          tagged
            te-1/1/2    FORWARDING    tagged
```

run show l3-interface

To display information about all L3 interfaces, use the **run show l3-interface** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface [brief | detail]

Parameters

Parameter	Description
brief	Optional. Show all L3 interfaces briefly.
detail	Optional. Show detail information of all L3 interfaces.

Example

- The following example displays information about all L3 interfaces.

```
admin@Switch# run show l3-interface
lo          Hwaddr E0:07:1B:C9:20:9B, Vlan:4095, MTU: 1500, State:UP
            Inet addr: fe80::e207:1b20:c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets................0

vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets................0

vlan100     Hwaddr E0:07:1B:C9:20:9B, Vlan:100, MTU: 1500, State:DOWN
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets................0
```

- This example shows all L3 interfaces briefly:

```
admin@XorPlus# run show l3-interface brief
Interface    Vlan ID    Status    Addr
---------    -------    ------    ------------------
lo           4095       UP        fe80::e207:1b20:c9:209b/64
vlan10       10         UP        10.1.1.166/24
                                  fe80::e207:1b20:1c9:209b/64
vlan100      100        DOWN
vlan1000     1000       UP        10.1.1.166/24
                                  fe80::e207:1b20:8c9:209b/64
```

run show l3-interface loopback

To display information about a L3 VLAN interface or loopback interface, use the **run show l3-interface loopback** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface loopback {**lo** | *<vrf-name>*}

Parameters

Parameter	Description
{**lo** | *<vrf-name>*}	Required parameter. Specifies VRF name. • **lo**: indicates the loopback interface in default VRF. • *<vrf-name>:* Specifies VRF name. The value is a string.

Example

- The following example displays information about the loopback interface in the default VRF:

```
admin@Switch# run show l3-interface loopback lo
lo          Hwaddr E0:07:1B:C9:20:9B, Vlan:4095, MTU: 1500, State:UP
            Inet addr: fe80::e207:1b20:c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets................0
```

run clear l3-interface statistics

This command clears the statistics information of L3 interface.

Command Syntax

run clear l3-interface statistics [**loopback** | <*vlan-interface*>]

Parameters

Parameter	Description
[**loopback** | <*vlan-interface*>]	Specifies the loopback interface or a VLAN interface.

Example

• This example clears the statistics information of loopback interface:

```
admin@XorPlus# run clear l3-interface statistics loopback
admin@XorPlus# commit
```

set l3-interface routed-interface dhcp

DHCP can be enable or disable on this routed interface or sub-interface as dhcp client. The routed interface or sub-interface will get ip address by DHCP server if DHCP is enable on this interface.

Command Syntax
set l3-interface routed-interface <*interface-name*> **dhcp** <*boolean*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
dhcp <*boolean*>	Enables or disables DHCP on a routed interface or sub-interface as DHCP client. The value include: • **true:** Enable DHCP client on routed interface or sub-interface. • **false:** Default configuration. Disable DHCP client on routed interface or sub-interface.

Example

- Enable DHCP client on routed interface.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 dhcp true
admin@XorPlus# commit
```

set l3-interface routed-interface rate-limit

The **set l3-interface routed-interface rate-limit** command configures the CPU egress rate limit for an L3 VLAN interface.

The **delete l3-interface routed-interface rate-limit** command deletes the CPU egress rate limit for a routed interface or a sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **rate-limit** <*rate-limit*>

delete l3-interface routed-interface <*interface-name*> **rate-limit**

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
rate-limit <*rate-limit*>	Specifies an egress rate limit for the L3 VLAN interface. The value is an integer, in kbps, that ranges from 1 to 1000000000. By default, there is no rate limit for the L3 VLAN interface in the outbound direction.

Usage Guidelines

Routed interface rate limit is applied to packets delivered out from the CPU, controlling shock of large flow of packets and releasing the burden on CPU.

Example

- Configure rate limit for a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 rate-limit 1024
admin@Xorplus# commit
```

set l3-interface routed-interface mtu

The **set l3-interface routed-interface mtu** command configures the maximum transmission unit (MTU) of a Layer 3 routed interface.

The **delete l3-interface routed-interface mtu** command deletes the IP MTU to the default value.

NOTE:

- The MTU value takes effect only on the outbound interface of the routed interface.
- It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.
- If you need to use IPv6 related functions, MTU needs at least 1280 bytes.

Command Syntax

set l3-interface routed-interface <*interface-name*> **mtu** <*mtu-value*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name. The value is a string.
mtu <*mtu-value*>	Specifies the MTU of an interface. The value is an integer that ranges from 68 to 65535, in bytes. The default value is 1500 bytes.

Usage Guidelines

An MTU value determines the maximum number of bytes in the IP layer packet that can be sent at a time. If the size of the data packets of the IP layer packet exceeds the MTU supported by a transit node or a receiver, the data packet is dropped at the sender's IP layer.

Example

- Configure the MTU for a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 mtu 2000
admin@Xorplus# commit
```

set l3-interface routed-interface vrf

The **set l3-interface routed-interface vrf** command is used to bind the layer 3 routed interface or sub-interface to the VRF.

Command Syntax

set l3-interface routed-interface<*interface-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

By binding the routed interfaces or sub-interfaces to different VRFs, the system segregates the IP routing table, ARP table, hardware forwarding table and host hardware forwarding table of different VRFs in customer edge devices.

Note that: The routed interfaces or sub-interfaces are in the default VRF if not explicitly bound to any VRF.

Example

• Bind the routed interface *rif-te4* to the VRF *vrf1*.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 vrf vrf1
admin@Xorplus# commit
```

set l3-interface routed-interface address

To configure an IPv4 or IPv6 address for an L3 interface, use the **set l3-interface routed-interface address** command in L2/L3 configuration mode. To remove an L3 interface, use the **delete** form of the command.

Command Syntax

set l3-interface routed-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>
delete l3-interface routed-interface <*interface-name*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
address	IPv4 or IPv6 address.
number	The network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Usage Guidelines

Layer 3 interfaces, including VLAN interface, loopback interface, routed interface and sub- interface, share the same hardware resources. When configuring IP address, it is required that the IP addresses of different layer 3 interfaces in the same VRF cannot be in the same subnet; However, overlapped layer 3 interface addresses in different VRFs is supported.

Example

- Configure the IPv4 address for a routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set l3-interface routed-interface rif-te4 address 10.10.0.1 prefix-length 24
admin@Xorplus# commit
```

- The following example configures the IPv6 address for the routed interface and then removes the L3 interface:

```
admin@Switch# set l3-interface routed-interface rif-te5 address 2001:1:1::1 prefix-length 64
admin@Switch# commit
admin@Switch# delete l3-interface routed-interface rif-te5
```

set l3-interface routed-interface description

The **set l3-interface routed-interface description** command configures the descriptive information for a routed interface or a sub-interface to help administrators and operators identify the purpose or role of an interface.

The **delete l3-interface routed-interface description** command deletes the descriptive information for a routed interface or a sub-interface.

Command Syntax

set l3-interface routed-interface<*interface-name*> **description** <*description*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
description <*description*>	Specifies a description for the interface. The value is a string.

Example

• Configure the description for a routed interface to *west*.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 description west
admin@Xorplus# commit
```

run show l3-interface routed-interface

The **run show routed interface** command shows the detailed layer 3 interface information of a specific routed interface or sub-interface.

Command Syntax

run show l3-interface routed-interface *<interface-name>*

Parameter

Parameter	Description
routed-interface *<interface-name>*	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- View the detailed layer 3 information of a specific routed interface.

```
admin@Xorplus# run show l3-interface routed-interface rif-te1
rif-te1          Hwaddr 18:5A:58:1F:63:A1, Vlan:800, MTU: 1500, State:UP
                 Inet addr: 120:1:1::49/64
                            fe80::1a5a:5820:131f:63a1/64
                 Traffic statistics:
                   5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
                   5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
                   IPv4 Input Packets.........................0
                   IPv4 Forwarding Packets....................0
                   IPv6 Input Packets.........................0
                   IPv6 Forwarding Packets....................0
```

set l3-interface vlan-interface pmtu-discovery

The **set l3-interface vlan-interface pmtu-discovery** command is used to enable or disable Path MTU(PMTU) function on a VLAN interface.

> **NOTE**:
>
> Enable PMTU function on all the nodes in the path where you want to apply the PMTU function.

The **delete l3-interface vlan-interface pmtu-discovery** command deletes the configuration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface*> **pmtu-discovery disable** <**true | false**>

Parameters

Parameter	Description
vlan-interface <*vlan-interface*>	Specifies the Layer 3 VLAN interface name. The value is a string.
disable <true | false>	Enables or disables the PMTU function. The value is **true** or **false**. • **true**: disables the PMTU function. • **false**: enables the PMTU function. By default, PMTU function is disabled.

Example

- Enable PMTU function on VLAN interface *vlan100*.

```
admin@PICOS# set l3-interface vlan-interface vlan100 pmtu-discovery disable false
admin@PICOS# commit
```

set l3-interface routed-interface pmtu-discovery

The **set l3-interface routed-interface pmtu-discovery** command is used to enable or disable Path MTU(PMTU) function on a routed interface.

> **NOTE**:
>
> Enable PMTU function on all the nodes in the path where you want to apply the PMTU function.

The **delete l3-interface routed-interface pmtu-discovery** command deletes the configuration.

Command Syntax

set l3-interface routed-interface <*routed-interface*> **pmtu-discovery disable** <**true | false**>

Parameters

Parameter	Description
routed-interface <*routed-interface*>	Specifies the Layer 3 routed interface name. The value is a string.
disable <true | false>	Enables or disables the PMTU function. The value is **true** or **false**. • **true**: disables the PMTU function. • **false**: enables the PMTU function. By default, PMTU function is disabled.

Example

- Enable PMTU function on routed interface *rif-te19*.

```
admin@PICOS# set l3-interface routed-interface rif-te19 pmtu-discovery disable false
admin@PICOS# commit
```

Routed Interface

- run show interface routed-interface brief
- run show vlans routed-vlan
- set interface aggregate-ethernet routed-interface enable
- set interface aggregate-ethernet routed-interface name
- set interface aggregate-ethernet routed-interface sub-interface vlan-id
- set interface gigabit-ethernet routed-interface enable
- set interface gigabit-ethernet routed-interface sub-interface
- set vlans reserved-vlan
- set interface gigabit-ethernet routed-interface name

run show interface routed-interface brief

The **run show interface routed-interface brief** command shows the brief information of the routed interfaces and sub-interfaces.

Command Syntax

run show interface routed-interface brief

Parameter

Null.

Example

- View the configuration information of routed interfaces and sub-interfaces.

```
admin@Xorplus# run show interface routed-interface brief
Interface       RoutedIfName     SubRoutedIfName  VLANID  Management  Status  Flow Control  Duplex  Speed    Descri
--------------  ---------------  ---------------  ------  ----------  ------  ------------  ------  -------  ------
te-1/1/1        rif-1                             800     Enabled     Up      Disabled      Full    1Gb/s
                                 rif-1.1          1102
                                 rif-1.2          1100
                                 rif-1.3          1101
te-1/1/2        rif-te2                           801     Disabled    Down    Disabled      Full    Auto
te-1/1/4        rif-te4                           802     Enabled     Down    Disabled      Full    Auto
te-1/1/5        rif-2                             803     Enabled     Up      Disabled      Full    2.5Gb/s
```

run show vlans routed-vlan

The **run show vlans routed-vlan** command shows the VLAN information of the routed interfaces and sub-interfaces.

Command Syntax

run show vlans routed-vlan

Parameter

Null.

Example

- View the VLAN information of the routed interfaces and sub-interfaces.

```
admin@Xorplus# run show vlans routed-vlan
VlanID  Vlan Name           Tag         Interfaces     Routed-interfaces
------  ------------------  --------    ------------   --------------------
800                         untagged    ge-1/1/5       rif-1
801                         untagged    ge-1/1/7       rif-2
1100    default             tagged      ge-1/1/5       rif-1.2
1101    default             tagged      ge-1/1/5       rif-1.3
1102    default             tagged      ge-1/1/5       rif-1.1
1103    default             tagged      ge-1/1/7       rif-2.1
```

The field "**Tag**" indicates whether the packets will be tagged or not when they are sent from this port.

set interface aggregate-ethernet routed-interface enable

The **set interface aggregate-ethernet routed-interface enable** command enables a LAG port as a layer 3 routed interface. LAG ports are layer 2 interfaces by default.

The **delete interface aggregate-ethernet routed-interface enable** command restores the LAG port to a layer 2 interface.

Command Syntax

set interface aggregate-ethernet *<lag-name>* **routed-interface enable <true | false>**

Parameter

Parameter	Description
aggregate-ethernet *<lag-name>*	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
enable <true | false>	Enables or disables the LAG port as a layer 3 routed interface. The value could be **true** or **false**. • **true**: Enables the LAG port as a layer 3 routed interface. • **false**: Disables the LAG port as a layer 3 routed interface. All LAG ports are layer 2 interfaces by default.

Example

- Enable the LAG port *ae3* as a layer 3 routed interface.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# commit
```

set interface aggregate-ethernet routed-interface name

The **set interface aggregate-ethernet routed-interface name** command configures the name for the routed interface, which will be referred to in other CLI commands as the routed interface name.

Command Syntax

set interface aggregate-ethernet <*lag-name*> **routed-interface name** <*string*>

Parameter

Parameter	Description
aggregate-ethernet <*lag-name*>	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
name <*string*>	Specifies the name for the routed interface. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Example

- Configure the name for the routed interface.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# commit
```

set interface aggregate-ethernet routed-interface sub-interface vlan-id

The **set interface aggregate-ethernet routed-interface sub-interface vlan-id** command creates a sub-interface and adds it into a VLAN. When creating a sub-interface, VLAN ID needs to be specified at the same time.

Command Syntax

set interface aggregate-ethernet *<lag-name>* **routed-interface sub-interface** *<sub-interface-name>* **vlan-id** *<vlan-id>*

Parameter

Parameter	Description
aggregate-ethernet *<lag-name>*	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
sub-interface <sub-interface-name>	Specifies the sub-interface name. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.
vlan-id *<vlan-id>*	Specifies the VLAN ID. The value is an integer that ranges from 2 to4094.

Example

- Create a sub-interface and add to VLAN 10.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface sub-interface rif-ae3.1 vlan-id 10
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface enable

The **set interface gigabit-ethernet routed-interface enable** command enables the Ethernet port as a layer 3 routed interface. All Ethernet ports are layer 2 interfaces by default.

The **delete interface gigabit-ethernet routed-interface enable** command restores the Ethernet port to a layer 2 interface.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface enable <true | false>**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
enable <true | false>	Enables or disables the Ethernet port as a layer 3 routed interface. The value could be **true** or **false**. • **true**: Enables the Ethernet port as a layer 3 routed interface. • **false**: Disables the Ethernet port as a layer 3 routed interface. All Ethernet ports are layer 2 interfaces by default.

Usage Guidelines

Pay attention to the following precautions before configuring a routed interface:

When enabling an Ethernet port/LAG interface as a layer 3 routed interface, a name for the routed interface should be configured by using the command **set interface gigabit-ethernet** <*interface-name*> **routed-interface name** <*string*>. This name will be referred to as the “interface name” in other CLI commands.

> **NOTE:**
> To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Reserved VLANs need to be configured on the device before configuring the routed interface.

Routed interface is mutually exclusive with the following layer 2 features, you have to delete all of the following configurations on the interface before enabling it as a routed interface, otherwise the routed interface commands will fail to commit.

set interface gigabit-ethernet <*interface-name*> **backup-port** *XX*
set interface aggregate-ethernet <*lag-name*> **backup-port** *XX*
set interface gigabit-ethernet <*interface-name*> **crossflow** *XX*
set interface aggregate-ethernet <*lag-name*> **crossflow** *XX*
set interface gigabit-ethernet <*interface-name*> **family** *XX*
set interface aggregate-ethernet <*lag-name*> **family** *XX*
set interface gigabit-ethernet <*interface-name*> **loopback true**
set interface gigabit-ethernet <*interface-name*> **port-security** *XX*
set interface aggregate-ethernet <*lag-name*> **port-security** *XX*
set interface gigabit-ethernet <*interface-name*> **static-ethernet-switching mac-address** *XX*
set interface aggregate-ethernet <*lag-name*> **static-ethernet-switching mac-address** *XX*
set interface gigabit-ethernet <*interface-name***> voice-vlan** *XX*
set interface aggregate-ethernet <*lag-name*> **voice-vlan** *XX*
set protocols dhcp snooping trust-port <*trust-port*>
set protocols igmp-snooping vlan-id <*vlan-id*> **mrouter interface** <*interface-name*>
set protocols igmp-snooping vlan-id <*vlan-id*> **static group** <*group-address*> **interface** <*interface-name*>
set protocols dot1x interface <*interface-name*>
set interface gigabit-ethernet <*interface-name*> **breakout true**

Besides the layer 2 features listed above, routed interface does not support Spanning Tree Protocol (STP) and MAC learning. However, the Layer 2 feature of LLDP is supported on an Ethernet port enabled as routed interface.

After a routed interface is enabled, you have to configure the following node to bring the routed interface up. Only after this, the corresponding sub-interfaces can be used normally.

set l3-interface routed-interface <*interface-name*>

The member port of a LAG port cannot be enabled as a routed interface, correspondingly, the physical port enabled as a routed interface cannot be configured as a LAG member port.

Example

- Enable the Ethernet port te-1/1/4 as a layer 3 routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface sub-interface

The **set interface gigabit-ethernet routed-interface sub-interface** command creates a sub-interface. When creating a sub-interface, VLAN ID needs to be specified at the same time.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
sub-interface <*sub-interface-name*>	Specifies the sub-interface name. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.
vlan-id <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 2 to 4094.

Usage Guidelines

Pay attention to the following precautions before configuring the sub-interfaces:

- Enable the Ethernet port as a routed interface before configuring the sub-interfaces.
- Define the VLAN ID by using the command **set vlans vlan-id** <*vlan-id*> before configuring the sub-interface and adding to VLAN.
- The IP address for each sub-interface should be in a different subnet from all the other sub-interfaces under that parent interface. That is, the IP subnets of all the sub-interfaces should be unique under the same parent interface.
- It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.
- On greyhound2 switches (including Dell N22xx series switches and N3208PX-ON), the sub-interface does not support user defined VRF and can only be used in the default VRF.
- The sub-interface of LAG port does not support user defined VRF and can only be used in the default VRF.

Example

- Create a sub-interface and add to VLAN 10.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface sub-interface rif-te4.1 vlan-id 10
admin@Xorplus# commit
```

set vlans reserved-vlan

The **set vlans reserved-vlan** command configures reserved VLANs for the use of routed interfaces.

Command Syntax

set vlans reserved-vlan *<reserved-vlan>*

Parameter

Parameter	Description
reserved-vlan *<reserved-vlan>*	Specifies the reserved VLANs. The valid VLAN numbers range is 2-4094. User can specify a range of VLAN numbers, e.g. 2,3,50-100. The system supports up to 128 reserved VLANs.

Usage Guidelines

Whenever a routed interface is configured, the system will automatically assign a VLAN internally to the routed interface from the reserved VLANs in order of smallest to largest.

The system supports up to 128 reserved VLANs.

VLAN 1 cannot be used as a reserved VLAN.

A reserved VLANs are VLANs dedicated to the routed interfaces (sub-interfaces are not included) and cannot be used for other interfaces, or other VLAN functions, such as PVLAN.

Reserved VLAN is mutually exclusive with the following settings, before configuring, please delete all these commands that uses the reserved VLAN, otherwise the reserved VLAN command will fail to commit.

set protocols dhcp snooping vlan *<vlan-id>*
set protocols igmp-snooping vlan-id *<vlan-id>*
set protocols dot1x block-vlan-id *<vlan-id>*
set protocols dot1x server-fail-vlan-id *<vlan-id>*
set vlans vlan-id *<vlan-id>* **private-vlan** *XX*

Note that: If you want to modify the value of the reserved VLANs, all the routed interfaces need to be disabled first.

You can use the commands **run show vlans** and **run show vlans routed-vlan** to check the VLAN information of all routed interfaces. For example,

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface name rif-te2
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set vlans reserved-vlan 80-85
admin@Xorplus# commit

admin@Xorplus# run show vlans
VlanID  Vlan Name           Tag        Interfaces
------  ------------------  --------   ----------------------------------------------------
1       default             untagged   te-1/1/1, xe-1/1/1, xe-1/1/2, xe-1/1/3, te-1/1/3
                                       xe-1/1/4, xe-1/1/5, te-1/1/5, xe-1/1/6, te-1/1/6
                                       te-1/1/7, te-1/1/8, te-1/1/9, te-1/1/10, te-1/1/11
                                       te-1/1/12, te-1/1/13, te-1/1/14, te-1/1/15, te-1/1/16
                                       te-1/1/17, te-1/1/18, te-1/1/19, te-1/1/20, te-1/1/21
                                       te-1/1/22, te-1/1/23, te-1/1/24, te-1/1/25, te-1/1/26
                                       te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30, te-1/1/31
                                       te-1/1/32, te-1/1/33, te-1/1/34, te-1/1/35, te-1/1/36
                                       te-1/1/37, te-1/1/38, te-1/1/39, te-1/1/40, te-1/1/41
                                       te-1/1/42, te-1/1/43, te-1/1/44, te-1/1/45, te-1/1/46
                                       te-1/1/47, te-1/1/48
                            tagged

80                          untagged   te-1/1/2
                            tagged

81                          untagged   te-1/1/4
                            tagged

82                          untagged
                            tagged
```

```
83                          untagged
                            tagged

84                          untagged
                            tagged

85                          untagged
                            tagged

admin@Xorplus# run show vlans routed-vlan
VlanID  Vlan Name           Tag         Interfaces     Routed-interfaces
------  ------------------  --------    ------------   --------------------
80                          untagged    te-1/1/2        rif-te2
81                          untagged    te-1/1/4        rif-te4
```

Example

- Configure reserved VLANs for the use of routed interfaces.

```
admin@Xorplus# set vlans reserved-vlan 800-900
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface name

The **set interface gigabit-ethernet routed-interface name** command configures the name for the routed interface, which will be referred to in other CLI commands as the routed interface name.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
name <*string*>	Specifies the name for the routed interface. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Example

- Configure the name for the routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# commit
```

set interface gigabit-ethernet speed

The **set interface gigabit-ethernet speed** command sets the force rate of an interface or enable auto-negotiation mode.

Command Syntax

set interface gigabit-ethernet<*interface-name*> **speed** [**auto** | <*speed*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name***>**	Specifies the interface name.
speed [**auto**	<*speed*>]	Specifies the interface rate. The values can be **auto** or <*speed*>. • **auto**: Sets the Ethernet interface to work in auto-negotiation mode. See Configuring the Auto-Negotiation Mode for details. • <*speed*>: Specifies an interface rate. The unit is **Mbit/s**. You can configure all rates of the parent interface and split interfaces, which are different based on different switch models. **NOTE**: If the rate you specified exceeds the maximum rate of the inserted optical module, the maximum rate of the optical module takes effect.

Usage Guidelines

Interface rate can be configured in the two modes: force rate (non-auto-negotiation mode) and auto-negotiation mode.

NOTEs:

- Interfaces at both ends of a link SHOULD work in the same auto-negotiation mode. Otherwise, the interfaces may not be able to communicate with each other.
- Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode. By default, these interfaces work in auto-negotiation mode. In auto-negotiation mode the ports negotiate any rate supported by the two devices. If the negotiated interface rate is not the required value, you can use the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate to make the interface negotiate the rate within the specified range.

Instructions for the switch interface rate configuration:

1. 1G RJ45 port: The interface rate can be configured to 100M, 10M or auto. By default, the interfaces work in auto-negotiation mode.
2. 1G optical port: The interface rate can be configured to 1000M or auto. By default, the interfaces work in auto-negotiation mode.
3. 10G RJ45 port: The interface rate can be configured to 100M or auto. By default, the interfaces work in auto-negotiation mode.
4. 10G optical port:

- When a 10G optical module is inserted, the interface rate can be configured to 10G or 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 10G.
- When a 1G optical module is inserted, the interface rate can be configured to 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 1G.

5. 40G optical port: The interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G or 1G.

6. 100G optical port:

- When a 100G optical module is inserted, the interface rate can be configured to 100G, 200G or 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 25G or 10G.
- When a 40G optical module is inserted, the interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G.

7. 200G optical port:

- When a 200G optical module is inserted, the interface rate can be configured to 200G,100G or 50G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 100G or 50G.
- When a 100G optical module is inserted, the interface rate can be configured to 100G,50G or 25G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 50G or 25G.

8. 400G optical port: The interface rate can be configured to 400G, 200G or 100G.

- When a 400G optical module is inserted, the interface rate can be configured to 400G, 200G or 100G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 200G or 100G.
- When a 200G optical module is inserted, the interface rate can be configured to 200G,100G or 50G. When no force rate is configured, the interface recognizes the interface rate of itself as 200G. If the interface configured interface split, the split interface rate can be configured to 100G or 50G.
- When a 100G optical module is inserted, the interface rate can be configured to 100G, 50G or 25G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 50G or 25G.

9. 800G optical port: Only 800G optical module can be inserted, and the interface rate can be configured to 800G, 400G, 200G or 100G. When no force rate is configured, the interface recognizes the interface rate of itself as 800G.

- If the interface configured interface split, the split interface rate can be configured to 400G, 200G or 100G.
- The speed of split interfaces can be further reduced by running the command **set interface gigabit-ethernet speed**. The reduced speed of split interfaces: 400G supports 200G and 100G; 200G supports 100G; 100G supports 50G.

Example

- Configure the force rate of the Te-1/1/49 port to 100Mbit/s.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/49 speed 100
admin@XorPlus# commit
```

Uplink Failure Detection Commands

- run show interface ufd
- set interface ufd link-to-monitor
- set interface ufd link-to-disable

run show interface ufd

The **run show interface ufd** command is used to view the uplink failure detection configuration information and status.

Command Syntax

run show interface ufd

Parameter

None.

Example

- View uplink failure detection configuration information and status.

```
admin@Xorplus# run show interface ufd
UFD: ufd1
-----------------------------------------------------
Uplink        : te-1/1/1 te-1/1/24
Downlink      : te-1/1/2 te-1/1/3
Failure Action: Inactive

UFD: ufd10
-----------------------------------------------------
Uplink        : te-1/1/10
Downlink      : te-1/1/11
Failure Action: Active
```

- If both the uplink and downlink interfaces are down, then the status of *Failure Action* is **Active** in the output. It means that uplink failure detection is working.
- If there is an uplink that is up, and hence that the downlink interface is also up, and that the status of *Failure Action* is **Inactive**.

set interface ufd link-to-monitor

The **set interface ufd link-to-monitor** command configures the uplink interface to an uplink failure detection group.

The **delete interface ufd link-to-monitor** command deletes the configuration.

Command Syntax

set interface ufd <*ufd-group-name*> **link-to-monitor** <*interface-name*>

Parameter

Parameter	Description
ufd <*ufd-group-name*>	Specifies the UFD group name. The value is a string in alpha-numeric format with no spaces.
link-to-monitor <*interface-name*>	Specifies the uplink interface to a UFD group. The value is a physical interface or a LAG interface.

Example

- Configure the uplink interface to an uplink failure detection group.

```
admin@Xorplus# set interface ufd ufd1 link-to-monitor ge-1/1/2
admin@Xorplus# commit
```

set interface ufd link-to-disable

The **set interface ufd link-to-disable** command configures the downlink interface to an uplink failure detection group.

The **delete interface ufd link-to-disable** command deletes the configuration.

Command Syntax

set interface ufd <*ufd-group-name*> **link-to-disable** <*interface-name*>

Parameter

Parameter	Description
ufd <*ufd-group-name*>	Specifies the UFD group name. The value is a string in alpha-numeric format with no spaces.
link-to-disable <*interface-name*>	Specifies the downlink interface to a UFD group. The value is a physical interface or a LAG interface.

Example

- Configure the downlink interface to an uplink failure detection group.

```
admin@Xorplus# set interface ufd ufd1 link-to-disable ge-1/1/3
admin@Xorplus# commit
```

IPv6 Neighbor Discovery Protocol Command Reference

This section describes the PICOS IPv6 Neighbor Discovery configuration commands.

> Please note that the N22XX series switches do not support IPv6.

- set l3-interface routed-interface ipv6-nd adv-interval-option
- set l3-interface routed-interface ipv6-nd home-agent-config-flag
- set l3-interface routed-interface ipv6-nd home-agent-lifetime
- set l3-interface routed-interface ipv6-nd home-agent-preference
- set l3-interface routed-interface ipv6-nd managed-config-flag
- set l3-interface routed-interface ipv6-nd mtu
- set l3-interface routed-interface ipv6-nd other-config-flag
- set l3-interface routed-interface ipv6-nd prefix off-link
- set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
- set l3-interface routed-interface ipv6-nd prefix router-address
- set l3-interface routed-interface ipv6-nd prefix valid-lifetime
- set l3-interface routed-interface ipv6-nd ra-fast-retrans
- set l3-interface routed-interface ipv6-nd ra-interval
- set l3-interface routed-interface ipv6-nd ra-lifetime
- set l3-interface routed-interface ipv6-nd reachable-time
- set l3-interface routed-interface ipv6-nd router-preference
- set l3-interface routed-interface ipv6-nd suppress-ra
- set l3-interface vlan-interface ipv6-nd adv-interval-option
- set l3-interface vlan-interface ipv6-nd home-agent-config-flag
- set l3-interface vlan-interface ipv6-nd home-agent-lifetime
- set l3-interface vlan-interface ipv6-nd home-agent-preference
- set l3-interface vlan-interface ipv6-nd managed-config-flag
- set l3-interface vlan-interface ipv6-nd mtu
- set l3-interface vlan-interface ipv6-nd other-config-flag
- set l3-interface vlan-interface ipv6-nd prefix off-link
- set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
- set l3-interface vlan-interface ipv6-nd prefix router-address
- set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
- set l3-interface vlan-interface ipv6-nd ra-fast-retrans
- set l3-interface vlan-interface ipv6-nd ra-interval
- set l3-interface vlan-interface ipv6-nd ra-lifetime
- set l3-interface vlan-interface ipv6-nd reachable-time
- set l3-interface vlan-interface ipv6-nd router-preference
- set l3-interface vlan-interface ipv6-nd suppress-ra

set l3-interface routed-interface ipv6-nd adv-interval-option

Run the command **set l3-interface routed-interface ipv6-nd adv-interval-option** to include the advertisement interval option in the RA packets. The Advertisement Interval Option indicates to host the maximum time in milliseconds between successive unsolicited Router Advertisements.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd adv-interval-option**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd adv-interval-option**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
adv-interval-option	Indicates the Ra packet advertisement interval option.

Example

- This example includes the advertisement interval option in RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd adv-interval-option
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-config-flag

Run the command **set l3-interface routed-interface ipv6-nd home-agent-config-flag** to set or unset the home agent config flag in RA packets. The Home Agent Option flag can be set or unset in IPv6 RA packets and is used to indicate to hosts that the router acts as Home Agent and includes a Home Agent Option. This option is not set by default.

Run the command **delete l3-interface routed-interface ipv6-nd home-agent-config-flag** to unset the flag.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-config-flag**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-config-flag	Indicates the home agent config flag in the RA packet.

Example

- This example command sets the home agent config flag in the RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-lifetime

Run the command **set l3-interface routed-interface ipv6-nd home-agent-lifetime** to set the home agent lifetime value in seconds. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the current Router Lifetime value.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-lifetime <***seconds*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-lifetime <***seconds*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-lifetime <*seconds*>	Specifies the home agent lifetime in seconds. The value is an integer that ranges from 0 to 65520. The default value is 0.

Example

- This example configures the home agent lifetime to 5 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-lifetime 5
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-preference

Run the command **set l3-interface routed-interface ipv6-nd home-agent-preference** to configure the home agent preference in RA packets. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the least preferred.

Run the command **delete l3-interface routed-interface ipv6-nd home-agent-preference** to delete this configuration and revert to the default value of 0.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-preference <***preference*>

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-preference <***preference*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-preference <*preference*>	Specifies the home agent preference. The value is an integer that ranges from 0 to 65535. The default value is 0.

Example

- This example configures the home agent preference to 5.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-preference 5
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd managed-config-flag

Run the command **set l3-interface routed-interface ipv6-nd managed-config-flag** to set or unset the managed config flag in the IPv6 RA packets. This flag indicates to the hosts that they must use managed protocol or stateful addresses autoconfiguration besides any addresses autoconfigured using stateless address autoconfiguration.

This flag is not set by default. To delete this configuration or unset the flag, run the command **delete l3-interface routed-interface ipv6-nd managed-config-flag.**

Command Syntax

set l3-interface routed-interface <*interface-name***> ipv6-nd managed-config-flag**

delete l3-interface routed-interface <*interface-name***> ipv6-nd managed-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- This example sets the managed config flag in the RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd managed-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd mtu

Run the command **set l3-interface routed-interface ipv6-nd mtu** to include the MTU option is RA packets. This option assists the hosts in proper interface configuration. The advertised MTU is not verified to be consistent with the actual router interface MTU.

Run the command **delete l3-interface routed-interface ipv6-nd mtu** to delete this option. This value is not configured in RA packets by default.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd mtu <***value*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd mtu**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
mtu <*value*>	Specifies the MTU value to advertise in RA packets. The value is an integer that ranges from 1 65535.

Example

- This example configures the advertised MTU value to 1000.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd mtu 1000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd other-config-flag

Run the command **set l3-interface routed-interface ipv6-nd other-config-flag** to set the *other config flag* in RA packets. This flag indicates to hosts that administered or stateful protocol should be used for autoconfiguration information other than addresses. This flag is not set by default.

Run the command **delete l3-interface routed-interface ipv6-nd other-config-flag** to unset this flag in RA packets.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd other-config-flag**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd other-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- This example sets the *other config flat* in RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd other-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix off-link

Run the command **set l3-interface routed-interface ipv6-nd prefix** to configure an IPv6 prefix to include in RA packets without specifying on-link or off-link properties of the advertised prefix. The off-link option is not set by default which means the prefix can be used for on-link determination. The optional parameter **no-autoconfig** can be used to indicate to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix** <*IPv6 Prefix*> **off-link [no-autoconfig]**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **off-link [no-autoconfig]**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
no-autoconfig	This option indicates to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Example

- This example configures an IPv6 prefix with off-link and no-autoconfig options.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 off-link no-autoconfig
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix preferred-lifetime

Run the command **set l3-interface routed-interface ipv6-nd prefix preferred-lifetime** to configure the advertised prefix preferred lifetime in seconds. Addresses generated from the prefix during this time period will be considered preferred addresses.

Run the command **delete l3-interface routed-interface ipv6-nd prefix preferred-lifetime** to remove this configuration.

Command Syntax

set l3-interface routed-interface *<interface-name>* **ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime <***seconds* **| infinite>**

delete l3-interface routed-interface *<interface-name>* **ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime**

Parameters

Parameter	Description
routed-interface *<interface-name>*	Specifies a routed interface name or sub-interface name. The value is a string.
prefix *<IPv6 Prefix>*	Specifies the IPv6 prefix, e.g. fa00::0/64
preferred-lifetime <*seconds* **| infinite>**	Specifies the time the addresses are treated as preferred addresses. The value could be in seconds from 0 to 4294967295 with default value of 604800 or use keyword **infinite** indicating infinity.

Example

- This example configures an IPv6 prefix with with infinite preferred lifetime.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 preferred-lifetime infinite
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix router-address

Run the command **set l3-interface routed-interface ipv6-nd prefix router-address** to set the R flag to indicate to hosts on local link that the specified prefix contains a complete IP address. This flag is not set by default which means hosts do not assume a complete IP address is placed.

Run the command **delete l3-interface routed-interface ipv6-nd prefix router-address** to unset this flag.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **router-address**

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **router-address**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64.

Example

- This example sets the R flag for the given prefix.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 router-address
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix valid-lifetime

Run the command **set l3-interface routed-interface ipv6-nd prefix valid-lifetime** to configure the time in seconds during which the prefix is considered valid for on-link determination.

Run the command **delete l3-interface routed-interface ipv6-nd prefix valid-lifetime** to delete this configuration and revert to the default value of 2592000 seconds.

Command Syntax

set l3-interface routed-interface *<interface-name>* **ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime <***seconds* **| infinite>**

delete l3-interface routed-interface *<interface-name>* **ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime**

Parameters

Parameter	Description
routed-interface *<interface-name>*	Specifies a routed interface name or sub-interface name. The value is a string.
prefix *<IPv6 Prefix>*	Specifies the IPv6 prefix, e.g. fa00::0/64
valid-lifetime <*seconds* **| infinite>**	Specifies the time period for which the prefix is valid. The value could be in seconds, Range: (0-4294967295) Default: 2592000. Or it could be **infinite** indicating infinite time.

Example

- This example configures the valid time of IPv6 prefix to infinity.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 valid-lifetime infinite
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-fast-retrans

Run the command **set l3-interface routed-interface ipv6-nd ra-fast-retrans** to enable or disable the IPv6 Router Advertisement fast retransmit feature. According to RFC4861, consecutive RA packets should be sent with at least 3 seconds delay. PICOS by default bypasses this restriction by fast transmission of RA to achieve better convergence.

Command Syntax

set l3-interface routed-interface *<interface-name>* **ipv6-nd ra-fast-retrans <true|false>**

Parameters

Parameter	Description
routed-interface *<interface-name>*	Specifies a routed interface name or sub-interface name. The value is a string.
ra-fast-retrans <true|false>	Enables or disables the Fast Retransmit feature. • **true:** Enables RA packet fast retransmit • **false:** Disables RA packet fast retransmit Default is enabled.

Example

- This example enables RA fast retransmit.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-fast-retrans true
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-interval

To set the RA interval, run the command **set l3-interface routed-interface ipv6-nd ra-interval**. This sets the time between unsolicited RA packets sent by the device on the specified interface. RA interval can be set in milliseconds or in seconds.

Run the command **delete l3-interface routed-interface ipv6-nd ra-interval** to remove this configuration and go back to the default interval of 60 seconds.

Command Syntax

set l3-interface routed-interface <*interface-name***> ipv6-nd ra-interval {sec <***seconds***> | msec <***milliseconds***>}**

delete l3-interface routed-interface <*interface-name***> ipv6-nd ra-interval {sec|msec}**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
sec <*seconds***>**	Specifies the interval in seconds, the value ranges from 1 to 1800 seconds. The default is 60 seconds.
msec <*milliseconds***>**	Specifies the interval in milliseconds, the value ranges from 70 to 1800000 milliseconds. The default value is 600000ms.

Example

- This example configures the RA interval to 50 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-interval sec 50
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-lifetime

Run the command **set l3-interface routed-interface ipv6-nd ra-lifetime** to configure the router lifetime field in the RA packets. This interval in seconds, indicate the effectiveness of the router on this link. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Command Syntax

set l3-interface routed-interface *<interface-name>* **ipv6-nd ra-lifetime <***seconds>*

delete l3-interface routed-interface *<interface-name>* **ipv6-nd ra-lifetime**

Parameters

Parameter	Description
routed-interface *<interface-name>*	Specifies a routed interface name or sub-interface name. The value is a string.
ra-lifetime <*seconds>*	Specifies the router lifetime interval in seconds. The value ranges from 0 to 9000. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Example

- This example configures an IPv6 router lifetime to 2000 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-lifetime 2000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd reachable-time

Run the command **set l3-interface routed-interface ipv6-nd reachable-time** to configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The command **delete l3-interface routed-interface ipv6-nd reachable-time** sets the reachable time to the default value of 0. (no limit).

Command Syntax

set l3-interfacerouted-interface <*interface-name*> **ipv6-nd reachable-time <***reachable-time*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd reachable-time**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
reachable-time <*reachable-time*>	Specifies the reachable time in milliseconds. The value ranges from 1 to 3600000. The default value is 0, indicating no limit.

Example

- This example configures an IPv6 reachable time to 2000 milliseconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd reachable-time 2000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd router-preference

Run the command **set l3-interface routed-interface ipv6-nd router-preference** to set the IPv6 Default Router Preference. Routers may include the default router preference in RA packets to signal to nodes the router preference in *low, medium* or *high.* Router preference is sent using the unused bits in the RA packet. The hosts that do not implement the default router preference will ignore these bits.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd router-preference <low|medium|high>**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd router-preference**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
router-preference <low|medium|high>	Specifies the default router preference, the three possible values are *low, medium* and *high.* • **low:** Specifies a low default router preference. • **medium:** Specifies a medium default router preference. • **high :** Specifies a high default router preference. The default is medium default router preference.

Example

- The command below sets the default router preference to low.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd router-preference low
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd suppress-ra

Run the command **set l3-interface routed-interface ipv6-nd supress-ra** to enable or disable sending Router Advertisement (RA) on the specified routed interface or sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd suppress-ra true**

set l3-interface routed-interface <*interface-name*> **ipv6-nd suppress-ra false**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
true	Disables sending RA packets.
false	This option enables sending RA packets.

Example

- This example enables sending RA packets on routed interface *rif-te4*.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd suppress-ra false
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd adv-interval-option

Run the command **set l3-interface vlan-interface ipv6-nd adv-interval-option** to include the advertisement interval option in the RA packets. The Advertisement Interval Option indicates to host the maximum time in milliseconds between successive unsolicited Router Advertisements.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd adv-interval-option**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd adv-interval-option**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
adv-interval-option	Indicates the Ra packet advertisement interval option.

Example

- This example includes the advertisement interval option in RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd adv-interval-option
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-config-flag** to set or unset the home agent config flag in RA packets. The Home Agent Option flag can be set or unset in IPv6 RA packets and is used to indicate to hosts that the router acts as Home Agent and includes a Home Agent Option. This option is not set by default.

Run the command **delete l3-interface vlan-interface vlan4001 ipv6-nd home-agent-config-flag** to unset the flag.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-config-flag**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-config-flag**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
home-agent-config-flag	Indicates the home agent config flag in the RA packet.

Example

- This example command sets the home agent config flag in the RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-lifetime** to set the home agent lifetime value in seconds. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the current Router Lifetime value.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-lifetime <***seconds***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-lifetime <***seconds***>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
home-agent-lifetime <*seconds*>	Specifies the home agent lifetime in seconds. The value is an integer that ranges from 0 to 65520. The default value is 0.

Example

- This example configures the home agent lifetime to 5 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-lifetime 5
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-preference

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-preference** to configure the home agent preference in RA packets. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the least preferred.

Run the command **delete l3-interface vlan-interface ipv6-nd home-agent-preference** to delete this configuration and revert to the default value of 0.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-preference <***preference***>**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-preference <***preference***>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
home-agent-preference <*preference***>**	Specifies the home agent preference. The value is an integer that ranges from 0 to 65535. The default value is 0.

Example

- This example configures the home agent preference to 5.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-preference 5
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd managed-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd managed-config-flag** to set or unset the managed config flag in the IPv6 RA packets. This flag indicates to the hosts that they must use managed protocol or stateful addresses autoconfiguration besides any addresses autoconfigured using stateless address autoconfiguration.

This flag is not set by default. To delete this configuration or unset the flag, run the command **delete l3-interface vlan-interface ipv6-nd managed-config-flag.**

Command Syntax

set l3-interface vlan-interface <*interface-name***> ipv6-nd managed-config-flag**

delete l3-interface vlan-interface <*interface-name***> ipv6-nd managed-config-flag**

Parameters

Parameter	Description
vlan-interface <*interface-name***>**	Specifies the VLAN interface name. The value is a string.

Example

- This example sets the managed config flag in the RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd managed-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd mtu

Run the command **set l3-interface vlan-interface ipv6-nd mtu** to include the MTU option is RA packets. This option assists the hosts in proper interface configuration. The advertised MTU is not verified to be consistent with the actual router interface MTU.

Run the command **delete l3-interface vlan-interface ipv6-nd mtu** to delete this option. This value is not configured in RA packets by default.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd mtu <***value***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd mtu**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
mtu <*value***>**	Specifies the MTU value to advertise in RA packets. The value is an integer that ranges from 1 65535.

Example

- This example configures the advertised MTU value to 1000.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd mtu 1000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd other-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd other-config-flag** to set the *other config flag* in RA packets. This flag indicates to hosts that administered or stateful protocol should be used for autoconfiguration information other than addresses. This flag is not set by default.

Run the command **delete l3-interface vlan-interface ipv6-nd other-config-flag** to unset this flag in RA packets.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd other-config-flag**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd other-config-flag**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.

Example

- This example sets the *other config flat* in RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd other-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix off-link

Run the command **set l3-interface vlan-interface ipv6-nd prefix** to configure an IPv6 prefix to include in RA packets without specifying on-link or off-link properties of the advertised prefix. The off-link option is not set by default which means the prefix can be used for on-link determination. The optional parameter **no-autoconfig** can be used to indicate to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix** <*IPv6 Prefix*> **off-link [no-autoconfig]**

delete l3-interface vlan-interface <*vlan-interface*> ipv6-nd prefix <*IPv6 Prefix***> off-link [no-autoconfig]**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
no-autoconfig	This option indicates to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Example

- This example configures an IPv6 prefix with off-link and no-autoconfig options.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 off-link no-autoconfig
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime** to configure the advertised prefix preferred lifetime in seconds. Addresses generated from the prefix during this time period will be considered preferred addresses.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix preferred-lifetime** to remove this configuration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime <***seconds* **| infinite>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
preferred-lifetime <*seconds* **| infinite>**	Specifies the time the addresses are treated as preferred addresses. The value could be in seconds from 0 to 4294967295 with default value of 604800 or use keyword **infinite** indicating infinity.

Example

- This example configures an IPv6 prefix with with infinite preferred lifetime.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 preferred-lifetime infinite
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix router-address

Run the command **set l3-interface vlan-interface ipv6-nd prefix router-address** to set the R flag to indicate to hosts on local link that the specified prefix contains a complete IP address. This flag is not set by default which means hosts do not assume a complete IP address is placed.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix router-address** to unset this flag.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> router-address**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> router-address**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64.

Example

- This example sets the R flag for the given prefix.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 router-address
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix valid-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd prefix valid-lifetime** to configure the time in seconds during which the prefix is considered valid for on-link determination.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix valid-lifetime** to delete this configuration and revert to the default value of 2592000 seconds.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime <***seconds* **| infinite>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
valid-lifetime <*seconds* **| infinite>**	Specifies the time period for which the prefix is valid. The value could be in seconds, Range: (0-4294967295) Default: 2592000. Or it could be **infinite** indicating infinite time.

Example

- This example configures the valid time of IPv6 prefix to infinity.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 valid-lifetime infinite
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-fast-retrans

Run the command **set l3-interface vlan-interface ipv6-nd ra-fast-retrans** to enable or disable the IPv6 Router Advertisement fast retransmit feature. According to RFC4861, consecutive RA packets should be sent with at least 3 seconds delay. PICOS by default bypasses this restriction by fast transmission of RA to achieve better convergence.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd ra-fast-retrans <true|false>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
ra-fast-retrans <true|false>	Enables or disables the Fast Retransmit feature. • **true:** Enables RA packet fast retransmit • **false:** Disables RA packet fast retransmit Default is enabled.

Example

- This example enables RA fast retransmit.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-fast-retrans true
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-interval

To set the RA interval, run the command **set l3-interface vlan-interface ipv6-nd ra-interval**. This sets the time between unsolicited RA packets sent by the device on the specified interface. RA interval can be set in milliseconds or in seconds.

Run the command **delete l3-interface vlan-interface ipv6-nd ra-interval** to remove this configuration and go back to the default interval of 60 seconds.

Command Syntax

set l3-interface vlan-interface <*interface-name***> ipv6-nd ra-interval {sec <***seconds***> | msec <***milliseconds***>}**

delete l3-interface vlan-interface <*interface-name***> ipv6-nd ra-interval {sec|msec}**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
sec <*seconds***>**	Specifies the interval in seconds, the value ranges from 1 to 1800 seconds. The default is 60 seconds.
msec <*milliseconds***>**	Specifies the interval in milliseconds, the value ranges from 70 to 1800000 milliseconds. The default value is 600000ms.

Example

- This example configures the RA interval to 50 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-interval sec 50
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd ra-lifetime** to configure the router lifetime field in the RA packets. This interval in seconds, indicate the effectiveness of the router on this link. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Command Syntax

set l3-interfacevlan-interface <*vlan-interface***> ipv6-nd ra-lifetime <***seconds***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd ra-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
ra-lifetime <*seconds***>**	Specifies the router lifetime interval in seconds. The value ranges from 0 to 9000. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Example

- This example configures an IPv6 router lifetime to 2000 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-lifetime 2000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd reachable-time

Run the command **set l3-interface vlan-interface ipv6-nd reachable-time** to configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The command **delete l3-interface vlan-interface ipv6-nd reachable-time** sets the reachable time to the default value of 0. (no limit).

Command Syntax

set l3-interfacevlan-interface <*vlan-interface***> ipv6-nd reachable-time <***reachable-time***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd reachable-time**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
reachable-time <*reachable-time***>**	Specifies the reachable time in milliseconds. The value ranges from 1 to 3600000. The default value is 0, indicating no limit.

Example

- This example configures an IPv6 reachable time to 2000 milliseconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd reachable-time 2000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd router-preference

Run the command **set l3-interface vlan-interface ipv6-nd router-preference** to set the IPv6 Default Router Preference. Routers may include the default router preference in RA packets to signal to nodes the router preference in *low, medium* or *high.* Router preference is sent using the unused bits in the RA packet. The hosts that do not implement the default router preference will ignore these bits.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd router-preference <low|medium|high>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd router-preference**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
router-preference <low|medium|high>	Specifies the default router preference, the three possible values are *low, medium* and *high.* • **low:** Specifies a low default router preference. • **medium:** Specifies a medium default router preference. • **high :** Specifies a high default router preference. The default is medium default router preference.

Example

- The command below sets the default router preference to low..

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd router-preference low
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd suppress-ra

Run the command **set l3-interface vlan-interface ipv6-nd supress-ra** to enable or disable sending Router Advertisement (RA) on the specified VLAN interface.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd suppress-ra true**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd suppress-ra false**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
true	Disables sending RA packets.
false	This option enables sending RA packets.

Example

- This example enables sending RA packets on interface vlan200.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd suppress-ra false
admin@XorPlus# commit
```

set management-ethernet-speed eth0

The **set management-ethernet-speed eth0** command configures port speed of **eth0** out-of-band management interface in operational mode.

Command Syntax

set management-ethernet-speed eth0 <**10 | 100 | 1000 | auto**>

Parameter

Null.

Example

- Configure port speed of **eth0** out-of-band management interface to 100Mbit/s and show the configuration result.

```
admin@PICOS> set management-ethernet-speed eth0 100
admin@PICOS> start shell sh
admin@PICOS:~$ sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  Not reported
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: No
        Advertised FEC modes: Not reported
        Speed: 100Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 2
        Transceiver: internal
        Auto-negotiation: off
        MDI-X: Unknown
```

set interface gigabit-ethernet up-mode

This command makes a local MAC layer to keep up status. This command generally coordinates with another command of interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean> when RX link of fiber breaks. If the two commands are configured together, TX link can still transmit traffic.

> **Caution:**
> Do not configure up-mode with UDLD, as this may cause the peer interface to be disabled unexpectedly by UDLD.

Command Syntax

set interface gigabit-ethernet <*port*> **up-mode** <*boolean*>

Parameter

<*port*> Ethernet port, now only support 10GE, 40GE, 100GE port .

<*boolean*> vaule is false or true. Default value is false.

Example

This example shows how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 up-mode true
admin@XorPlus# commit
```

show interface bpdu-tunneling

This command is to show bpdu tunneling on all interface.

Command Syntax
run show interface bpdu-tunneling

Example
• This example is to show bpdu tunneling:

```
admin@XorPlus# run show interface bpdu-tunneling
Destination Mac: 1:e:0:0:0:1
```

show interface aggregate-ethernet <lag_name>

This command is to show information about the specified LAG interface.

Command Syntax
run show interface aggregate-ethernet *<lag_name> [text]*

Parameter
•*<lag_name>* Name of LAG interface.
• [*text*] The special information. Options include:

- **brief** Show brief information
- **detail** Show detail information

Example
• This example is to show information of ae1:

```
admin@XorPlus# run show interface aggregate-ethernet ae1
Physical interface: ae1, Enabled, error-discard False, Physical link is Down
Interface index: 53
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.....................0
Output Packets....................0
Input Octets......................0
Output Octets.....................0
Aggregated link protocol: STATIC
Minimum number of selected ports: 1
Members Status Port Speed
--------- ---------- ----------
```

show interface aggregate-ethernet <lag_name> dot1q-tunneling

This command is to show dot1q-tunneling on a specified LAG.

Command Syntax
run show interface aggregate-ethernet *<lag_name>* dot1q-tunneling

Parameter
•*<lag_name>* Name of LAG interface.

Example
• This example is to show bpdu tunneling:

```
admin@XorPlus# run show interface aggregate-ethernet ae1 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
```

show interface brief

This command show interface brief information ,this information includes Interface name, Management,Status, Flow Control, Duplex ,Speed ,Description.

Command Syntax
run show interface brief

Example
• This example is to show brief information of interface.

```
admin@Xorplus#  run show interface brief
Interface       Management  Status  Flow Control  Duplex  Speed    Description
--------------  ----------  ------  ------------  ------  -------  ------------------------------
ge-1/1/1        Enabled     Down    Disabled      Full    Auto
ge-1/1/2        Enabled     Down    Disabled      Full    Auto
ge-1/1/3        Enabled     Down    Disabled      Full    Auto
ge-1/1/4        Enabled     Down    Disabled      Full    Auto
ge-1/1/5        Enabled     Down    Disabled      Full    Auto
ge-1/1/6        Enabled     Down    Disabled      Full    Auto
ge-1/1/7        Enabled     Down    Disabled      Full    Auto
ge-1/1/8        Enabled     Down    Disabled      Full    Auto
ge-1/1/9        Enabled     Down    Disabled      Full    Auto
ge-1/1/10       Enabled     Down    Disabled      Full    Auto
ge-1/1/11       Enabled     Down    Disabled      Full    Auto
ge-1/1/12       Enabled     Down    Disabled      Full    Auto
ge-1/1/13       Enabled     Down    Disabled      Full    Auto
ge-1/1/14       Enabled     Down    Disabled      Full    Auto
ge-1/1/15       Enabled     Down    Disabled      Full    Auto
ge-1/1/16       Enabled     Down    Disabled      Full    Auto
ge-1/1/17       Enabled     Down    Disabled      Full    Auto
ge-1/1/18       Enabled     Down    Disabled      Full    Auto
ge-1/1/19       Enabled     Down    Disabled      Full    Auto
ge-1/1/20       Enabled     Down    Disabled      Full    Auto
ge-1/1/21       Enabled     Down    Disabled      Full    Auto
ge-1/1/22       Enabled     Down    Disabled      Full    Auto
ge-1/1/23       Enabled     Down    Disabled      Full    Auto
ge-1/1/24       Enabled     Down    Disabled      Full    Auto
ge-1/1/25       Enabled     Down    Disabled      Full    Auto
ge-1/1/26       Enabled     Down    Disabled      Full    Auto
ge-1/1/27       Enabled     Down    Disabled      Full    Auto
ge-1/1/28       Enabled     Down    Disabled      Full    Auto
ge-1/1/29       Enabled     Down    Disabled      Full    Auto
ge-1/1/30       Enabled     Down    Disabled      Full    Auto
ge-1/1/31       Enabled     Up      Disabled      Full    1Gb/s
ge-1/1/32       Enabled     Up      Disabled      Full    1Gb/s
ge-1/1/33       Enabled     Down    Disabled      Full    Auto
ge-1/1/34       Enabled     Down    Disabled      Full    Auto
ge-1/1/35       Enabled     Down    Disabled      Full    Auto
ge-1/1/36       Enabled     Down    Disabled      Full    Auto
ge-1/1/37       Enabled     Down    Disabled      Full    Auto
ge-1/1/38       Enabled     Down    Disabled      Full    Auto
ge-1/1/39       Enabled     Down    Disabled      Full    Auto
ge-1/1/40       Enabled     Down    Disabled      Full    Auto
ge-1/1/41       Enabled     Down    Disabled      Full    Auto
ge-1/1/42       Enabled     Down    Disabled      Full    Auto
ge-1/1/43       Enabled     Down    Disabled      Full    Auto
ge-1/1/44       Enabled     Down    Disabled      Full    Auto
ge-1/1/45       Enabled     Down    Disabled      Full    Auto
ge-1/1/46       Enabled     Down    Disabled      Full    Auto
ge-1/1/47       Enabled     Down    Disabled      Full    Auto
ge-1/1/48       Enabled     Down    Disabled      Full    Auto
te-1/1/1(49)    Enabled     Up      Disabled      Full    10Gb/s
te-1/1/2(50)    Enabled     Down    Disabled      Full    10Gb/s
```

The number (49), (50) with the interface name are the physical port labels of the interface.

show interface detail

This command show interface detail information.

Command Syntax
run show interface detail

Example
• This example is to show detail information of interface :

```
admin@XorPlus# run show interface detail
Physical interface: ge-1/1/1, Enabled, error-discard False, Physical link is Up
Interface index: 1, SFP type: Unknown
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 100Mb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:100, egress:100
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 392 bits/sec, 0 packets/sec
Input Packets.........................99114129
Output Packets........................57388
Input Octets.........................6343304256
Output Octets........................7021889
Transmit:
Unicast packets.....................0
Multicast packets.....................57388
Broadcast packets.....................0
Packets 64 Octets.....................0
Packets 65-127 Octets.................55264
Packets 128-255 Octets................2124
Packets 256-511 Octets................0
Packets 512-1023 Octets...............0
Packets 1024-1518 Octets..............0
Oversize Packets.....................0
Total Packets Without Errors..........57388
Discarded Packets.....................0
Total Packets With Errors.............0
Single Collision Frames...............0
Multiple Collision Frames.............0
Deferred Frames.......................0
Late Collisions.......................0
Excessive Collisions..................0
Pause Frames..........................0
Receive:
Unicast packets.....................99114129
-More-
```

show interface diagnostics optics all

This command is to show diagnostics informations of all interface or a specified interface.

Command Syntax
run show interface diagnostics optics [**all** | <*interface-name*>]

Example
• This example is to show diagnostics informations:

```
admin@Xorplus# run show interface diagnostics optics all
Interface       Temp(C/F)    Voltage(V)  Bias(mA)  Tx Power(dBm)  Rx Power(dBm)  Module Type
--------------  -----------  ----------  --------  -------------  -------------  -----------
te-1/1/1(49)    27.78/82.00  3.27        6.88      -3.38          -20.00         10G_BASE_SR


admin@Xorplus# run show interface diagnostics optics te-1/1/1
Interface       Temp(C/F)    Voltage(V)  Bias(mA)  Tx Power(dBm)  Rx Power(dBm)  Module Type
--------------  -----------  ----------  --------  -------------  -------------  -----------
te-1/1/1(49)    27.78/82.00  3.27        6.88      -3.38          -20.00         10G_BASE_SR
```

The number (49) with the interface name is the physical port label of the interface.

show interface ecmp max-path

This command is to show max counter of ecmp path.

Example
• This example is to show max counter of ecmp path:

```
admin@XorPlus# run show interface ecmp max-path
max-path:   4
```

show interface flexlink

This command is to show flexlink information.

Command Syntax
run show interface flexlink

Example
• This example is to show flexlink on all interfaces:

```
admin@XorPlus# run show interface flexlink
Active Interface Backup Interface Mode Delay(seconds)
---------------- ---------------- --------- --------------
ge-1/1/1(up) ge-1/1/2(standby) off 0
```

show interface gigabit-ethernet <interface>

This command is to show brief,detail or dot1q-tunneling information of a specified port.

Command Syntax
run show interface gigabit-ethernet *<interface> [text]*

Parameter
•*<interfce>* a specified interface identifier,[ge-1/1/1...ge-1/1/48],[te-1/1/49...te-1/1/52]
•*[text]* The special information.

- **brief** Show interface brief information
- **detail** Show interface detail information
- **dot1q-tunneling** Show dot1q tunneling information about the specified interface

Example
• This example is to show detail information on ge-1/1/3:

```
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/3 detail
Physical interface: ge-1/1/3, Enabled, error-discard False, Physical link is Up
Interface index: 3, SFP type: Unknown, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 100Mb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:0, egress:0
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 392 bits/sec, 0 packets/sec
Input Packets.............................10000
Output Packets............................186601
Input Octets..............................640000
Output Octets............................15763131
Transmit:
Unicast packets.......................91800
Multicast packets.....................64781
Broadcast packets.....................30020
Packets 64 Octets.....................121822
Packets 65-127 Octets.................64777
Packets 128-255 Octets.................2
Packets 256-511 Octets.................0
Packets 512-1023 Octets................0
Packets 1024-1518 Octets...............0
Oversize Packets.......................0
Total Packets Without Errors...........186601
Discarded Packets......................0
Total Packets With Errors..............0
Single Collision Frames................0
Multiple Collision Frames..............0
Deferred Frames........................0
Late Collisions........................0
Excessive Collisions...................0
Pause Frames...........................0
Receive:
Unicast packets.......................10000
Multicast packets.....................0
Broadcast packets.....................0
Packets 64 Octets.....................10000
Packets 65-127 Octets.................0
Packets 128-255 Octets.................0
Packets 256-511 Octets.................0
Packets 512-1023 Octets................0
Packets 1024-1518 Octets...............0
Oversize Packets.......................0
```

```
Total Packets Without Errors..........10000
Discarded Packets.....................0
Total Packets With Errors.............0
Alignment Errors......................0
FCS Errors............................0
Collisions............................0
Pause Frames..........................0



admin@Xorplus# run show interface gigabit-ethernet te-1/1/1
Physical interface: te-1/1/1(49), Enabled, error-discard False, Physical link is Up
Interface index: 49, SFP+ type: 10G_BASE_SR, Mac Learning Enabled
Description:
Link-level type: Ethernet, MTU: 1518, Speed: 10Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Disabled
Interface flags: SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Link fault signaling  ignore local fault:false, ignore remote fault:false
force up mode:true
Precision Time Protocol mode:none
Current address: 1c:72:1d:c9:1b:e1, Hardware address: 1c:72:1d:c9:1b:e1
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 1607765248 bits/sec, 2450861 packets/sec
  Input Packets.........................0
  Output Packets.......................17156180968
  Input Octets..........................0
  Output Octets........................1406807017424
```

set interface gigabit-ethernet fec

The **set interface gigabit-ethernet fec** command is used to enable or disable Forwarding Error Correction (FEC) function on the 100G, 40G or 25G port of the switch.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **fec** <**true | false**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the 100G, 40G or 25G interface name of the switch.
fec <**true	false**>	Enable or disable FEC function. The value could be **true** or **false**. • **true**: enables FEC function. • **false**: disables FEC function. By default, FEC function is disabled.

Example

- Disable FEC function on the switch port xe-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/1 fec false
admin@XorPlus# commit
```

- Enable FEC function on the switch port xe-1/1/2.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/2 fec true
admin@XorPlus# commit
```

set interface gigabit-ethernet family ethernet-switching vlan members

This command is to add a vlan member to this trunk port with tagged packet, vlan members range from 1 to 4094. The default of this command is that packets are tagged when the packets go out from this interface.

Note: If this interface's native-vlan-id is identical to vlan-member, packets will be encapsulated with vlan tag because tagged packet is the default configuration of vlan-member.

Command Syntax
set interface gigabit-ethernet *<port>* **family ethernet-switching vlan members** *<vlan-id>*
delete interface gigabit-ethernet *<port>* **family ethernet-switching vlan members** *<vlan-id>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.

• *<vlan-id>* Configure the VLAN ID or VLAN ID range for which the interface can carry traffic, eg: 2, 3... Range: 1 to 4094.

> **NOTE:**
> When configuring VLAN member, use VLAN ID or VLAN range, but NOT other strings.

Example

• This example is adding a trunk port (ge-1/1/3) to a VLAN:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 5
admin@XorPlus# commit
```

• This example is adding a trunk port (ge-1/1/30) to a VLAN range:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/30 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/30 family ethernet-switching vlan members 50-100
admin@XorPlus# commit
```

• This example is adding a trunk port (te-1/1/30) to VLAN 2 and 3:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/30 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/30 family ethernet-switching vlan members 2,3
admin@XorPlus# commit
```

set interface gigabit-ethernet family ethernet-switching port-mode

The **set interface gigabit-ethernet family ethernet-switching port-mode** command configures the port mode of a switch port.

Command Syntax

set interface gigabit-ethernet <*interface-name*> f**amily ethernet-switching port-mode** <*port-mode*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3.
port-mode <*port-mode*>	Specifies the port mode. The value could be **access**, **trunk**, **pvlan-host**, **pvlan-secondary-trunk**, **pvlan-promiscuous** or **pvlan-promiscuous-trunk**. • **access**: Configures the port mode to access. • **trunk**: Configures the port mode to trunk. • **pvlan-host**: Configures the port mode to pvlan-host. • **pvlan-secondary-trunk**: Configures the port mode to pvlan-secondary-trunk. • **pvlan-promiscuous**: Configures the port mode to pvlan-promiscuous. • **pvlan-promiscuous-trunk**: Configures the port mode to pvlan-promiscuous-trunk. By default, the port mode is access.

Usage Guidelines

There are six port modes, the last four of these modes are used for PVLAN. Only when configured with a PVLAN port mode, a port can be added into a private VLAN.

NOTE:

After modifying the port mode, the port will be restarted automatically.

The characteristics of different port modes:

- Access Port

An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. An access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the native VLAN ID.

- Trunk Port

A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- PVLAN Host Port

A PVLAN host port connects to a user device. For host mode ports, make sure that their native VLAN is a secondary VLAN, otherwise the ports won't be able to forward packets from primary VLAN. One host port can be added into only one secondary VLAN.

Packets sent from this port are untagged.

- PVLAN Secondary Trunk Port

A PVLAN secondary trunk port is used to connect to the downstream devices. One secondary trunk port can be added into more than one secondary VLAN. Secondary trunk mode is applicable to scenarios where multiple secondary VLANs need to pass through the downlink port while Host mode is applicable to cases where only one secondary VLAN passes through the downlink port.

The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the secondary trunk mode port, thus masking the primary VLAN for the downstream device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

NOTE:

- Secondary trunk mode ports can be added to only one secondary VLAN of the same primary VLAN, but can be added to multiple secondary VLANs associated with different primary VLANs.
- PVLAN secondary trunk port can also be added to normal VLANs in addition to the secondary VLANs.

- PVLAN Promiscuous Port

PVLAN promiscuous ports are used to connect to the uplink devices. Uplinks are typically ports that connect to routers, firewalls, servers or provider networks.

Promiscuous ports belong to the primary VLAN, which can communicate with all PVLAN ports, including host/secondary trunk ports and other promiscuous/promiscuous trunk ports within the same primary VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.

Make sure that the native VLAN of the promiscuous port is the primary VLAN, otherwise the port will not forward packets sent from a secondary VLAN.

Promiscuous port mode is used when there is only one primary VLAN passing through the uplink port. Packets sent from this port are untagged.

- PVLAN Promiscuous Trunk Port

PVLAN promiscuous trunk ports are used to connect to the uplink devices. Promiscuous trunk port mode is used when there are more than one primary VLAN passing through the uplink port.

The secondary VLAN ID carried by the message is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the uplink device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> PVLAN Promiscuous trunk ports can also be added to normal VLANs in addition to the primary VLANs.

Example

- Configure the port mode of ge-1/1/1 to access.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode access
admin@Xorplus# commit
```

set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol

The **set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol** command enables the BPDU tunneling function of the Layer 2 protocol.

Command Syntax

set interface gigabit-ethernet *<port-id>* **family ethernet-switching bpdu-tunneling protocol** *<protocol-type>*

Parameter

Parameter	Description
gigabit-ethernet *<port-id>*	Specifies switch port identifier. Note: BPDU Tunneling cannot be configured on a LAG port, or the physical port that belongs to a LAG. When you need to configure BPDU tunneling on the physical port that belongs to a LAG, you need to first take the physical port out of the LAG port before configuration.
protocol *<protocol-type>*	Specifies the Layer 2 protocol, which needs to be transmitted through BPDU tunnel. The values could be **STP** or **LACP**.

Example

• Enable the BPDU tunneling function of STP protocol.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching bpdu-tunneling protocol stp
admin@XorPlus# commit
```

set interface gigabit-ethernet ether-options 802.3ad

The **set interface gigabit-ethernet ether-options 802.3ad** command adds a specified port to a LAG.

Command Syntax
set interface gigabit-ethernet <*interface-name***> ether-options 802.3ad** *<lag-interface-name>*
delete interface gigabit-ethernet <*interface-name***> ether-options 802.3ad**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name***>**	Specifies the ethernet switching port identifier which will be added to the LAG interface.
<lag-interface-name>	Specifies the name of the LAG interface. The value is a string in the format of **ae***x*. **Note**: The maximum LAGs per switch is limited by the interface capacity.

NOTE:

The maximum number of member ports per LAG is platform dependent, for details see Collection of Feature Specification of Different Platforms.

Example
• This example is to add ge-1/1/3 to ae1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae1
admin@XorPlus#commit
```

set interface gigabit-ethernet duplex auto

The **set interface gigabit-ethernet duplex auto** command configures the duplex mode of optical port as auto negotiation mode.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **duplex auto**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the optical port name.

Usage Guidelines

Pay attention to the following notes:

- Currently, duplex mode for optical port is only available for the 10 optical port when its port rate set to 1G.
- Duplex mode for optical port currently only supports to configure as auto, i.e. auto negotiation mode.
- It is required that the duplex mode of the peer 1G optical port is also set to auto negotiation mode, otherwise the port cannot link up.

Use command **delete interface gigabit-ethernet** <*interface-name*> **duplex** to go back to the default duplex mode to full.

Example

- Set the duplex mode of optical port te-1/1/1 as auto negotiation mode.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 speed 1000
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 duplex auto
```

set interface gigabit-ethernet breakout-type

The **set interface gigabit-ethernet breakout-type** command can specify the breakout type as four 100G, two 200G, four 50G, two 100G or four 25G based on different switch models.

NOTEs:

- To cancel the split configuration of an interface, use **set interface gigabit-ethernet** <*port-name*> **breakout false** command to restore the split interfaces to one interface.
- If you enable the breakout function of interface without configuring the breakout-type, the 400GE interface will be split into four 100G Ethernet interfaces and the 200GE interface will be split into four 50G Ethernet interfaces by default.
- The interface name is modified after port breakout or merge, you need to manually delete the configurations of the unavailable interfaces before restarting system, to make sure that the configuration file can be loaded normally when system boots up.

Command Syntax

set interface gigabit-ethernet <*port-name*> **breakout-type** {**4*100G** | **2*200G**}

set interface gigabit-ethernet <*port-name*> **breakout-type** {**4*100G | 2*200G | 4*50G | 2*100G | 4*25G**}

Parameter

Parameter	Description
gigabit-ethernet <*port-name*>	Specifies the name of a 400G or 200G interface.
breakout-type {**4*100G** | **2*200G**}	Specifies the breakout type as four 100G or two 200G for switches supporting 400G interfaces.
breakout-type {**4*100G** | **2*200G	4*50G	2*100G	4*25G**}	Specifies the breakout type as four 100G, two 200G, four 50G, two 200G or four 25G for switches (N8550-24CD8D) supporting 400G and 200G interfaces. • For 400G interface, when you specify the breakout type as 2*200G or 4*100G: ◦ The interface will be split into two 200GE interfaces or four 100GE interfaces with 400G optical module inserted. ◦ the interface will be split into two 100GE interfaces or four 50GE interfaces with 200G optical module inserted. ◦ The interface will be split into two 50GE interfaces or four 25GE interfaces with 100G optical module inserted. • For 200G interfaces:

	◦ When you specify the breakout type as 2*100G or 4*50G, the interface will be split into two 100GE interfaces or four 50GE interfaces with 200G optical module inserted. ◦ When you specify the breakout type as 4*25G, the interface will be split into four 25GE interfaces with 100G optical module inserted. ◦ When you specify the breakout type as 2*100G, the interface will be split into two 50GE interfaces with 100G optical module inserted.

Example

- Split the 400GE interface xe-1/1/26 into four 100G Ethernet interfaces.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/26 breakout true
admin@PICOS# set interface gigabit-ethernet xe-1/1/26 breakout-type 4*100G
admin@PICOS# commit
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading startup configuration will fail.
admin@PICOS# exit
admin@PICOS> start shell sh
admin@PICOS:~$ sudo systemctl restart picos
```

set interface gigabit-ethernet auto-speeds

The **set interface gigabit-ethernet auto-speeds** command sets the auto-negotiation rate of an interface in auto-negotiation mode.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **auto-speeds** <*auto-speed*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name***>**	Specifies the interface name.
auto-speeds <*auto-speed***>**	Specifies the auto-negotiation rate, the unit is **Mbit/s**. • For 1G RJ45port, the values of auto-negotiation rate could be 1000M, 100M or 10M. • For 10G RJ45 port, the values of auto-negotiation rate could be 10000M, 1000M or 100M. • For 5G/2.5G RJ45 port, the values of auto-negotiation rate could be 100M, 1000M, 2500M, 5000M and 10000M.

Usage Guidelines

NOTE:

- Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode and auto-negotiation rate.
- The auto-negotiation rates configured on the interfaces must have an intersection at both ends of the link.

Run the **set interface gigabit-ethernet**<*interface-name*> **speed auto** command to configure the Ethernet interface to work in auto-negotiation mode before using the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate.

Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode. By default, these interfaces work in auto-negotiation mode. In auto-negotiation mode the ports negotiate any rate supported by the two devices. If the negotiated interface rate is not the required value, you can use the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate to make the interface negotiate the rate within the specified range.

Example

- Set the auto-negotiation rates of ge-1/1/1 interface to 100M and 10M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 100
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 10
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

- Set the auto-negotiation rates of ge-1/1/1 interface to 1000M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 1000
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

set interface ecmp hash-mapping field vlan disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." User can also enable additional fields like vlan.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field vlan disable *<bool>*
delete interface ecmp hash-mapping field vlan disable

Parameter
•*<bool>* disable including the field

- **true** disable vlan
- **false** enable vlan. Default.

Example
• This example is to enable vlan:

```
admin@XorPlus# set interface ecmp hash-mapping field vlan disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field port-source disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." User can also enable additional fields like port-source.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field port-source disable *<bool>*
delete interface ecmp hash-mapping field port-source disable

Parameter
•*<bool>* disable including the field

- **true** disable port-source
- **false** enable port-source. Default.

Example
• This example is to enable port-source:

```
admin@XorPlus# set interface ecmp hash-mapping field port-source disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field port-destination disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like port-destination.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field port-destination disable <*bool*>
delete interface ecmp hash-mapping field port-destination disable

Parameter
•<*bool*> disable including the field

- **true** disable port-destination
- **false** enable port-destination. Default.

Example
• This example is to enable port-destination:

```
admin@XorPlus# set interface ecmp hash-mapping field port-destination disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-source disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-source.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-source disable *<bool>*
delete interface ecmp hash-mapping field ip-source disable

Parameter
•*<bool>* disable including the field

- **true** disable ip-source
- **false** enable ip-source. Default.

Example
• This example is to enable ip-source:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-source disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-protocol disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-protocol.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-protocol disable <*bool*>
delete interface ecmp hash-mapping field ip-protocol disable

Parameter
•<*bool*> disable including the field

- **true** disable ip-protocol
- **false** enable ip-protocol. Default.

Example
• This example is to enable ip-protocol:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-protocol disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-destination disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-destination.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-destination disable *<bool>*
delete interface ecmp hash-mapping field ip-destination disable

Parameter
•*<bool>* disable including the field

- **true** disable ip-destination
- **false** enable ip-destination. Default.

Example
• This example is to enable ip-destination:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-destination disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ingress-interface disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ingress-interface.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ingress-interface disable *<bool>*
delete interface ecmp hash-mapping field ingress-interface disable

Parameter
•*<bool>* disable including the field

- **true** disable ingress-interface
- **false** enable ingress-interface. This is the default value.

Example
• This example is to enable ingress interface:

```
admin@XorPlus# set interface ecmp hash-mapping field ingress-interface disable false
admin@XorPlus# commit
```

set interface bpdu-tunneling destination-mac

The **set interface bpdu-tunneling destination-mac** command configures the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

Command Syntax

set interface bpdu-tunneling destination-mac <*destination-mac*>

Parameter

Parameter	Description
destination-mac <*destination-mac*>	Specifies the destination multicast MAC address that replaces the destination multicast MAC address of Layer 2 protocol packets. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The value ranges from 01:00:00:00:00:00 to 01:ff:ff:ff:ff:ff. The following multicast MAC addresses can not be used: 01:80:C2:00:00:00 to 01:80:C2:00:00:2f.

Example
• Configures the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

```
admin@XorPlus# set interface bpdu-tunneling destination-mac 01:90:00:00:00:1a
admin@XorPlus# commit
```

set interface aggregate-ethernet family ethernet-switching vlan members

This command is to add a vlan member to the trunk lag, vlan members range from 1 to 4094. The default of this command is that packets are tagged when the packets go out from this interface.

Note: If this interface's native-vlan-id is identical to vlan-member, packets will be encapsulated with vlan tag because the " tagged" is the default configuration of vlan-member.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **family ethernet-switching vlan members** *<vlan-id>*
delete interface aggregate-ethernet *<lag_name>* **family ethernet-switching vlan members** *<vlan-id>*

Parameter
• *<lag_name>* Name of a LAG interface.
• *<vlan-id>* Configure the VLAN ID or VLAN ID range for which the interface can carry traffic, eg: 2, 3... Range: 1 to 4094.

> **NOTE:**
> When configuring VLAN member, use VLAN ID or VLAN range, but NOT other strings.

Example

• This example is adding a trunk LAG port (ae1) to a VLAN:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 5
admin@XorPlus# commit
```

• This example is adding a trunk LAG port (ae1) to a VLAN range:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 50-100
admin@XorPlus# commit
```

• This example is adding a trunk LAG port (ae1) to VLAN 2 and 3:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 2,3
admin@XorPlus# commit
```

set interface aggregate-ethernet family ethernet-switching port-mode

The **set interface aggregate-ethernet family ethernet-switching port-mode** command configures the port mode of a switch LAG interface.

Command Syntax
set interface aggregate-ethernet <*lag-interface-name*> **family ethernet-switching port-mode** <*port-mode*>
delete interface aggregate-ethernet <*lag-interface-name*> **family ethernet-switching port-mode**

Parameter

Parameter	Description
aggregate-ethernet <*lag-interface-name*>	Specifies a LAG interface name. The value is like ae1, ae2.
port-mode <*port-mode*>	Specifies the port mode. The value could be **access**, **trunk**, **pvlan-host**, **pvlan-secondary-trunk**, **pvlan-promiscuous** or **pvlan-promiscuous-trunk**. • **access**: Configures the port mode as access. • **trunk**: Configures the port mode as trunk. • **pvlan-host**: Configures the port mode as pvlan-host. • **pvlan-secondary-trunk**: Configures the port mode as pvlan-secondary-trunk. • **pvlan-promiscuous**: Configures the port mode as pvlan-promiscuous. • **pvlan-promiscuous-trunk**: Configures the port mode to pvlan-promiscuous-trunk. By default, the port mode is access.

Usage Guidelines

There are six port modes, the last four of these modes are used for PVLAN. Only when configured with a PVLAN port mode, a port can be added into a private VLAN.

NOTE:

After modifying the port mode, the port will be restarted automatically.

The characteristics of different port modes:

- **Access Port**

An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. An access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the native VLAN ID.

- **Trunk Port**

A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- **PVLAN Host Port**

A PVLAN host port connects to a user device. For host mode ports, make sure that their native VLAN is a secondary VLAN, otherwise the ports won't be able to forward packets from primary VLAN. One host port can be added into only one secondary VLAN.

Packets sent from this port are untagged.

- **PVLAN Secondary Trunk Port**

A PVLAN secondary trunk port is used to connect to the downstream devices. One secondary trunk port can be added into more than one secondary VLAN. Secondary trunk mode is applicable to scenarios where multiple secondary VLANs need to pass through the downlink port while Host mode is applicable to cases where only one secondary VLAN passes through the downlink port.

The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the secondary trunk mode port, thus masking the primary VLAN for the downstream device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

NOTE:

- Secondary trunk mode ports can be added to only one secondary VLAN of the same primary VLAN, but can be added to multiple secondary VLANs associated with different primary VLANs.
- PVLAN secondary trunk port can also be added to normal VLANs in addition to the secondary VLANs.

- **PVLAN Promiscuous Port**

PVLAN promiscuous ports are used to connect to the uplink devices. Uplinks are typically ports that connect to routers, firewalls, servers or provider networks.

Promiscuous ports belong to the primary VLAN, which can communicate with all PVLAN ports, including host/secondary trunk ports and other promiscuous/promiscuous trunk ports within the same primary VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.

Make sure that the native VLAN of the promiscuous port is the primary VLAN, otherwise the port will not forward packets sent from a secondary VLAN.

Promiscuous port mode is used when there is only one primary VLAN passing through the uplink port. Packets sent from this port are untagged.

- **PVLAN Promiscuous Trunk Port**

PVLAN promiscuous trunk ports are used to connect to the uplink devices. Promiscuous trunk port mode is used when there are more than one primary VLAN passing through the uplink port.

The secondary VLAN ID carried by the message is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the uplink device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> PVLAN Promiscuous trunk ports can also be added to normal VLANs in addition to the primary VLANs.

Example

• This example sets ae1 port mode to trunk:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# commit
```

set interface aggregate-ethernet disable

Enable or disable a LAG interface.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **disable** <true | false>

To delete the configuration enter:

delete interfaceaggregate-ethernet <*lag_name*> **disable**

Parameter

- <*lag_name*> Name of a LAG interface.
- true: disable a logical interface
- false: enable a logical interface

Example

This example disables the ae1 interface:

```
admin@XorPlus# set interface aggregate-ethernet ae1 disable true
admin@XorPlus# commit
```

set interface aggregate-ethernet description

Use this command to add a description to a LAG port.

Command Syntax
set interface aggregate-ethernett <*lag_name*> **description** <*description*>

To delete the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **description**

Parameter
• <*lag_name*> Name of LAG interface.
• <*description*> Add a human-readable description of the interface

Example
This example adds the description *hello* to port named ae1.

```
admin@XorPlus# set interface aggregate-ethernet ae1 description hello
admin@XorPlus# commit
```

set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout

The **set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout** command configures the LACP fallback timer.

Command Syntax

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback timeout** <*timer*>

Parameters

Parameter	Description
aggregate-ethernet <*lag-interface*>	Specifies the LAG interface name. The value is a string like ae1, ae99 and so on. NOTE: LACP fallback can only be applied on the LACP LAG interface, but not on a static LAG.
timeout <*timer*>	Specifies the timer to bring up a LAG and keeps one member port active. The value is an integer. The default value is 10 seconds.

Example

- Configure LACP fallback timer to 20 seconds.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback timeout 20
```

set interface aggregate-ethernet aggregated-ether-options lacp fallback enable

The **set interface aggregate-ethernet aggregated-ether-options lacp fallback enable** command can be used to enable or disable LACP fallback mode on a LAG interface.

Command Syntax

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback enable** <**true | false**>

Parameters

Parameter	Description
aggregate-ethernet <*lag-interface*>	Specifies the LAG interface name. The value is a string like ae1, ae99 and so on. **NOTE:** LACP fallback can only be applied on the LACP LAG interface, but not on a static LAG.
enable <**true	false**>	Enable or disable LACP fallback feature. • **true**: Enable LACP fallback feature. • **false**: Disable LACP fallback feature.

Example

- Enable LACP fallback feature on LAG interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback enable true
```

set interface aggregate-ethernet aggregated-ether-options lacp

Creates a Link Aggregation Control Protocol (LACP) link aggregation group (LAG) on a specified LAG port.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **aggregated-ether-options lacp enable** <true | false>

To return the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **aggregated-ether-options lacp**

Parameter

- *<lag_name>* Enter the name of the LAG.
- true: enable LACP
- false: disable LACP

Example

This example configures LACP for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@XorPlus# commit
```

set interface aggregate-ethernet

Use this command to create a Link Aggregation Group (LAG) interface.

Command Syntax

set interface aggregate-ethernet *<lag_name>*

Parameter

<lag_name> Enter the name of the LAG interface.

NOTE:

Before PicOS 2.9.2, the maximum number of LAGs is 48 on all models, that is, PicOS supports to configure LAG as ae1 to ae48 on all models.

In PicOS 2.9.2 and the later versions, the maximum number of LAGs is equal to the maximum number of physical interfaces by each model from ae1.

The maximum number of LAGs varies by platform, for details see Collection of Feature Specification of Different Platforms.

Example

The example creates a LAG named **ae4**.

```
admin@XorPlus# set interface aggregate-ethernet ae4
admin@XorPlus# commit
```

run show interface port-index-mapping

The **run show interface port-index-mapping** command shows the mapping informations between Logical Port Index and Physical Port Label.

Command Syntax
run show interface port-index-mapping

Example
• This example shows the interface mapping informations between the Logical Port Index and Physical Port Label.

Column "**Logical Port Index**" is logical interface name, "**Physical Port Label**" is same as the panel number of the physical port.

```
admin@Xorplus# run show interface port-index-mapping
Logical Port Index  Physical Port Label
------------------  -------------------
ge-1/1/1            1
ge-1/1/2            2
ge-1/1/3            3
ge-1/1/4            4
ge-1/1/5            5
ge-1/1/6            6
ge-1/1/7            7
ge-1/1/8            8
ge-1/1/9            9
ge-1/1/10           10
ge-1/1/11           11
ge-1/1/12           12
ge-1/1/13           13
ge-1/1/14           14
ge-1/1/15           15
ge-1/1/16           16
ge-1/1/17           17
ge-1/1/18           18
ge-1/1/19           19
ge-1/1/20           20
ge-1/1/21           21
ge-1/1/22           22
ge-1/1/23           23
ge-1/1/24           24
ge-1/1/25           25
ge-1/1/26           26
ge-1/1/27           27
ge-1/1/28           28
ge-1/1/29           29
ge-1/1/30           30
ge-1/1/31           31
ge-1/1/32           32
ge-1/1/33           33
ge-1/1/34           34
ge-1/1/35           35
ge-1/1/36           36
ge-1/1/37           37
ge-1/1/38           38
ge-1/1/39           39
ge-1/1/40           40
ge-1/1/41           41
ge-1/1/42           42
ge-1/1/43           43
ge-1/1/44           44
ge-1/1/45           45
ge-1/1/46           46
ge-1/1/47           47
ge-1/1/48           48
te-1/1/1            49
te-1/1/2            50
te-1/1/3            51
```

```
te-1/1/4            52
xe-1/1/1            53
xe-1/1/2            54
```

run show interface diagnostics tdr

The **run show interface diagnostics tdr** command.

Command Syntax

run show interface diagnostics tdr *<interface-name>*

Parameter

Parameter	Description
tdr *<interface-name>*	Specifies interface name of Ethernet electrical interface.

Example

- Run the following command to start the TDR cable test. The following example shows the cable length (Pair length) is approximately 31 meters long with a possible error of +/- 10 meters. All four pairs are working fine (Pair status).

```
admin@Xorplus# run show interface diagnostics tdr ge-1/1/1
Interface  Local pair Pair length(meter) Remote pair Pair status
---------- ---------- ------------------ ----------- -----------
ge-1/1/1   Pair A     31   +/- 10        Pair A      OK
           Pair B     31   +/- 10        Pair B      OK
           Pair C     31   +/- 10        Pair C      OK
           Pair D     30   +/- 10        Pair D      OK
```

Table 2. Description of the run show interface diagnostics tdr output

Item	Description
Interface	Indicates the name of the interface on which TDR test is enabled.
Local pair	Local four pairs.
Pair length(meter)	Displays the length and error of the cable pair in meters. • When the pair is not faulty, the Pair length in the displayed message refers to the total length of the pair. • When the pair is faulty, the Pair length in the displayed message is the length from the interface to the fault point in the cable.
Remote pair	Remote four pairs.
Pair status	The pair status could be "**OK**", "**OPEN**", "**SHORT**", "**OPENSHORT**", "**CROSSTALK**" or "**N/A**". • **OK**: indicates the link is up. • **OPEN**: indicates an open circuit, meaning a broken wire or maybe cable unplugged. • **SHORT**: indicates there is a short circuit on the cable. • **N/A**: indicates the port does not support TDR test.

interface max-route-limit

This command is to set max route count .

Command Syntax
set interface max-route-limit <*counter*>
delete interface max-route-limit

Parameter
•<*counter*> Max Route Counter,range is [0..12000]

Example
• This example is to set max route counter 12 and delete it:

```
admin@XorPlus# set interface max-route-limit 12
admin@XorPlus# delete interface max-route-limit
admin@XorPlus# commit
```

interface max-acl-rule-limit <egress/ingress>

This command is to set max acl rule counter .

Command Syntax
set interface max-acl-rule-limit <*egress/ingress*> <acl-counter>
delete interface max-acl-rule-limit egress
delete interface max-acl-rule-limit ingress

Parameter
• <*egress/ingress*> the in/out mode of a port

- **egress** Set max egress acl rule count
- **ingress** Set max ingress acl rule count

•<*acl-counter*> max egress or ingress acl counter identifier. Egress:,the counter is [0..256].ingress:[0..896]

Example
• This example is to max ingress ACL counter is 400

```
admin@XorPlus# set interface max-acl-rule-limit ingress 400
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> min_thresh

Users can set minimum thresh.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> min_thresh <*int*>
delete interface gigabit-ethernet <*port*> wred queue <*value*> min_thresh

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The threshold identifier,[0..8000]

Example
• This example sets max thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 min_thresh 1
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> max_thresh

Users can set max thresh.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> max_thresh <*int*>
delete interface gigabit-ethernet <*port*> wred queue <*value*> max_thresh

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The threshold identifier,[0..8000]

Example
• This example sets max thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 max_thresh 100
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> enable

Users can set wred queue when necessary.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> enable <*bool*>
delete interface gigabit-ethernet <*port*> wred queue <*value*> *enable*

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*bool*> Set enable

- **true** enable wred
- **false** disable wred

Example
• This example sets wred queue for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 enable true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> ecn_thresh

Users can set ecn_thresh.

Command Syntax
set interface gigabit-ethernet *<port>* wred queue *<value>* ecn_thresh *<int>*
delete interface gigabit-ethernet *<port>* wred queue 2 ecn_thresh

Parameter
• *<port>*ethernet switching port identifier,the valid ports range 1-52
•*<value>* The queue number,[0..7]
•*<int>* The threshold identifier,[0..1],0 stands for disable ecn,1 stands for enable ecn.

Example
• This example sets ecn_thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 ecn_thresh 0
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> drop_probability

Users can set drop_probability.

Command Syntax
set interface gigabit-ethernet *<port>* wred queue *<value>* drop_probability *<int>*
delete interface gigabit-ethernet <port> wred queue *<value>* drop_probability

Parameter
• *<port>*ethernet switching port identifier,the valid ports range 1-52
•*<value>* The queue number,[0..7]
•*<int>* The probability identifier,[0...100]

Example
• This example sets wred queue drop probability for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 drop_probability 10
admin@XorPlus# commit
```

interface gigabit-ethernet <port> storm-control <mode> ratio <value>

Users can set storm control mode for a specified port. The storm control function can control the rate of ingress traffic on the physical port. The ratio value is the percentage of the physical link speed.

Command Syntax
set interface gigabit-ethernet *<port>* storm-control *<mode>ratio <value>*
delete interface gigabit-ethernet *<port>* storm-control broadcast ratio

Parameter
• *<port>* ethernet port
• *<mode>* packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for all multicast traffic
- **unicast** Storm control for unknown unicast traffic

•*<value> range is* [0..100]. This value is percentage of the physical link speed. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast, multicast, unicast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast ratio 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control multicast ratio 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control unicast ratio 30
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

interface gigabit-ethernet <port> storm-control <mode> pps

Users can set storm control mode for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> storm-control <*mode*> pps <*value*>
delete interface gigabit-ethernet <*port*> storm-control [<*mode*> | **pps**]

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Packets per second, [0..30000000]. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast pps 1000
admin@XorPlus# commit
```

interface gigabit-ethernet <port> storm-control <mode> kbps

Users can set storm control mode for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> **storm-control** <*mode*> **kbps** <*value*>
delete interface gigabit-ethernet <*port*> **storm-control** [<*mode*> | **kbps**]

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Kilo bits per second, [0..10000000]. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast kbps 1000
admin@XorPlus# commit
```

interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>

User can configure a mac address for port belong to more than one vlan.

Command Syntax
set interface gigabit-ethernet <*port*> static-ethernet-switching mac-address <*mac-address*> vlan <*vlan-id*>

Parameter
• <*port*> GigabitEthernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1, ae1.
• <*mac-address*> Add static mac address for a specific interface.
• <*vlan-id*> VLAN tag identifier, the valid VLAN numbers range 1-4094, can create specify a range of VLAN numbers, e.g. 2,3,5-100.

Example
• This example configures a mac address for port belong to vlan 1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 static-ethernet-switching mac-address 22:11:11:11:11:11 vla
admin@XorPlus# commit
```

interface gigabit-ethernet <port> snmp-trap

Users can eable or disable snmp trap when necessary.

Command Syntax
set interface gigabit-ethernet <*port*> snmp-trap <*bool*>
delete interface gigabit-ethernet <*port*> snmp-trap

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*bool*> Snmp trap when port link up and down

- **true** enable snmp-trap
- **false** disable snmp-trap

Example
• This example enable snmp-trap for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 snmp-trap true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> power-preemphasis-level

Users can set power-preemphasis-level for a port .

Command Syntax
set interface gigabit-ethernet <*port*> power-preemphasis-level <*value*>
delete interface gigabit-ethernet <*port*> power-preemphasis-level

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*value*>the level identifier, [0..15]

Example
• This example set preemphasis-level 3 for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 power-preemphasis-level 3
admin@XorPlus# commit
```

interface gigabit-ethernet <port> mtu

Users can set maximum transmit packet size for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> mtu <*value*>
delete interface gigabit-ethernet <*port*> mtu

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52
• <*value*> maximum transmit packet size identifier(in octets),value is between [64..9216]

Example
• This example sets MTU 1024 for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 mtu 1024
admin@XorPlus# commit
```

interface gigabit-ethernet <port> mac-learning <boolean>

This command function is setting if the port could learn the source mac address of ingress packet.

Command Syntax
set interface gigabit-ethernet <*port*> mac-learning <*boolean*>
delete interface gigabit-ethernet <*port*> mac-learning

Parameter
• <*port*> Ethernet switching port identifier
•<*boolean*> True or False. The default value is true. False value is the port can't learn the source mac address when packet is enterring the port. True value is the port can learn the source mac address.

Example
• This example configures the port ge-1/1/1 mac-learning false:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 mac-learning false
admin@XorPlus# commit
```

interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>

When local RS receive remote fault messages, local RS will inhibit transmission of frames.

These commands determine if local RS would ignore remote fault messages to permit transmission of frames when receiving remote fault messages.

Command Syntax

set interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>.

Parameter

<port> Ethernet physical interface, now only support 10GE, 40GE, 100GE port .

<boolean> Vaule is false or true. Default value is false.

Example

This example is how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-remote-fault true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>

A fiber has two links, TX and RX. When RX link failure occurs, local fault messages are generated by PHY layer to RS layer. As soon as RS receives a local fault message, it will generate Remote fault messages and transmit Remote fault messages to remote RS through TX link. RS is the only layer that can generate Remote fault messages.

This command determines if local RS would ignore local fault message to generate Remote fault messages when RX link failure occurs. This command generally coordinates with another command of interface gigabit-ethernet <port> up-mode <boolean> when RX link of fiber breaks. If the two commands are configured together, TX link can still transmit traffic.

Command Syntax

set interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>

Parameter

• *<port>* Ethernet port, now only support 10GE, 40GE, 100GE port .

•*<boolean> Vaule is* false or true. Default value is false.

Example

• This example is how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-local-fault true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged

This command is to add a vlan member to the trunk port with untagged packet, vlan members range from 1 to 4094. When packets go out from this interface, the field of vlan tag will be removed from the packet.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching vlan members *<vlan-id> untagged*
delete interface gigabit-ethernet *<port>* family ethernet-switching vlan members *<vlan-id>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• *<vlan-id>* Configure vlan id for which the interface can carry traffic,eg:2,3...

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 5 untagged
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching native-vlan-id

The native VLANID is the ID of the default VLAN (usually vlan-id 1) in which the the port belongs. User can change the native VLANID for port.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching native-vlan-id <*vlan-id*>
delete interface gigabit-ethernet <*port*> family ethernet-switching native-vlan-id <*vlan-id*>

Parameter
• <*port*> Gigabit Ethernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1.
• <*vlan_id*> The native-vlan-id ,VLAN identifier to associate with untagged packets .the valid VLAN numbers range 1-4094.

Example
• This example creates VLAN 3 and puts ge-1/1/3 port on this VLAN:

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode

Users can configure a Q-in-Q tunnel mode for a port. By default, the mode is NONE.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling mode *[mode]*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• *[mode]* Q-in-Q tunnel mode.

- **internal** Flexible QinQ: service provider internal mode
- **external** Basic QinQ: customer to service provider mode
- **none** Disable tunneling mode,the **default** mode

Example
• This example is to set Q-in-Q tunnel mode for ge-1/1/3 port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress

Users can configure/delete a Q-in-Q tunnel for entering traffic on a port.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling ingress *<text>*
delete interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling ingress *<text>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• *<text>*Tunneling for entering traffic

Example
• This example is to configure a Q-in-Q tunnel for entering traffic:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type

Users can set/delete a Ethertype value on Q-in-Q tunnel for a port.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling ether-type *<value>*
delete interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling ether-type *<value>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• <value> Ethertype value

- **0x8100**
- **0x88a8**
- **0x9100**
- **0x9200**

Example
• This example is to select a Ethertype value on Q-in-Q tunnel for ge-1/1/3 port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching dot1q-tunneling ether-type 0x8100
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress

Users can configure/delete a Q-in-Q tunnel for exiting traffic on a port.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling egress *<text>*
delete interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling egress *<text>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• *<text>*Tunneling for existing traffic

Example
• This example is to configure a Q-in-Q tunnel for existing traffic:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching dot1q-tunneling egress t2
admin@XorPlus# commit
```

interface gigabit-ethernet <port> disable

User can enable or disable an interface.

Command Syntax
set interface gigabit-ethernet *<port>* disable *<bool>*
delete interface gigabit-ethernet *<port>* disable

Parameter
• *<bool>* up/down an interface

- **true** disable an interface
- **false** enable an interface

Example
• This example is to disable ge-1/1/3 interface:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 disable true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> ether-options flow-control

Flow control is a mechanism used on Ethernet networks to slow the flow of traffic to prevent a receiving node from becoming overwhelmed. Implemented at the data link layer, it enables such a receiving node to send a message to other relevant switches or hosts to slow their data transfer rate. Ethernet flow control was originally implemented to address cases where network interface controllers (NICs) lacked sufficient buffer space to keep up with traffic flows. Today, it's more likely to be used to address network congestion in a switch, such as when traffic comes in over a higher speed link than the one where it goes out. It can also be useful when traffic is coming in from multiple high-speed connections and threatens to fill the switch buffer. This document details how to configure flow control on Gigabit Ethernet ports on a white box switch running the Pica8 PICOS network operating system.

Command Syntax
set interface gigabit-ethernet <*port*> ether-options flow-control <*bool*>
delete interface gigabit-ethernet <*port*> ether-options flow-control

Parameter
• <port> ethernet switching port identifier,the valid ports range 1-52
• <*bool*> enable flow control

- **true** enable flow control
- **false** disable flow control. This is default configuration.

Example
• This example is to configure ge-1/1/3 port in flow control:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options flow-control true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> description

Users can add a description to a port.

Command Syntax
set interface gigabit-ethernet <*port*> description <*text*>
delete interface gigabit-ethernet <*port*> description

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52
• <*text*> Add a human-readable description of the interface

Example
• This example is to add description "hello" to ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 description hello
admin@XorPlus# commit
```

interface gigabit-ethernet <port> crossflow local-control

User can configure a crossflow port in local-control mode or not.

Command Syntax
set interface gigabit-ethernet <*port*> crossflow local-control <*bool*>
delete interface gigabit-ethernet <*port*> crossflow local-control

Parameter
• <*port*> a physical port or a LAG
• <*bool*> set local control

- **true** enable local control,**default** mode
- **false** disable local control

Example
• This example is to configure a croosflow port ge-1/1/3 not in local control:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow local-control false
admin@XorPlus# commit
```

interface gigabit-ethernet <port> crossflow enable

User can configure a specified port in crossflow mode or not.

Command Syntax
set interface gigabit-ethernet <*port*> crossflow enable <*bool*>
delete interface gigabit-ethernet <*port*> crossflow enable

Parameter
• <*port*> a physical port or a LAG
• <*bool*> Enable crossflow

- **true** enable crossflow
- **false** disable crossflow

Example
• This example is to configure ge-1/1/3 port in croosflow port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow enable true
admin@XorPlus#commit
```

interface gigabit-ethernet <port> backup-port mode

User can set preemption mode of a port.

Command Syntax
set interface gigabit-ethernet *<port>* backup-port mode *<mode>*
delete interface gigabit-ethernet *<port>* backup-port mode

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
•*<mode>* Set preemption mode.

- **bandwidth** higher bandwidth interface preferred
- **forced** active interface preferred,the **default** mode
- **Off** turn off preemption

Example
• This example is to set the port preemption mode to bandwidth:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 backup-port mode bandwidth
admin@XorPlus# commit
```

interface gigabit-ethernet <port> backup-port interface

User can configure two physical ports or two LAGs as Flex Links, or one physical port and one LAG as Flex Links.

Command Syntax
set interface gigabit-ethernet *<port>* backup-port interface *<text>*
delete interface gigabit-ethernet *<port>* backup-port interface

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
•*<text>* Set backup port of an interface, which will disable rstp/mstp

Example
• This example is to set Flex links between a physical port and a LAG :

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 backup-port interface ae1
admin@XorPlus# commit
```

interface gigabit-ethernet <port> backup-port delay

User can set backup port delay time to a port.

Command Syntax
set interface gigabit-ethernet <*port*> backup-port delay <*seconds*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
•<*seconds*> preemption delay in seconds,range is [0..300]

Example
• This example is to set the delay time to 20s:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 backup-port delay 20
admin@XorPlus# commit
```

interface ethernet-switching-options mac-table-aging-time

Users can configure the aging time of mac table

Command Syntax
set interface ethernet-switching-options mac-table-aging-time <*value*>
Delete interface ethernet-switching-options mac-table-aging-time

Parameter
• <*value*> Aging time in seconds, the range is [60..1000000].

Example
• This example is to configure the aging time (60)of mac table :

```
admin@XorPlus# set interface ethernet-switching-options mac-table-aging-time 60
admin@XorPlus# commit
```

interface ethernet-switching-options buffer queue-limit

interface ethernet-switching-options buffer queue-limit
User can set the limit value of queue buffer.

Command Syntax
set interface ethernet-switching-options buffer queue-limit <*value*>
delete interface ethernet-switching-options buffer queue-limit

Parameter
• <*value*>the queue-limit values indentifier,ranges from 0 to 20000

Example
• This example is to configure the buffer queue limit:

```
admin@XorPlus# set interface ethernet-switching-options buffer queue-limit 0
admin@XorPlus# delete interface ethernet-switching-options buffer queue-limit
admin@XorPlus#commit
```

interface ecmp max-path

This command is to set max counter of ecmp path.

Command Syntax
set interface ecmp max-path <*value*>
delete interface ecmp max-path

Parameter
•<*value*> Max of ecmp path

- **2**
- **4**
- **8**
- **16**
- **32**

Example
• This example is to set max of ecmp path 2:

```
admin@XorPlus# set interface ecmp max-path 2
admin@XorPlus# commit
```

interface cut-through-mode

Pica8 switch has two switching modes. One is store and-forward mode， another is cut-through mode.

By default, the switch forwards the packets in store and forward mode. Users can configure the switch to cut-through mode .

Command Syntax
set interface cut-through-mode <*bool*>
delete interface cut-through-mode

Parameter
• <*bool*> forwarding mode identifier

- **true** interface is in cut-through mode
- **false** interface is in store and forward mode

Example
• This example is to configure the interface in store and forward mode

```
admin@XorPlus# set interface cut-through-mode false
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
XorPlus#
```

interface aggregate-ethernet <lag_name> storm-control <mode> pps

Users can set storm control mode for a specified port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **storm-control** <*mode*> **pps** <*value*>
delete interface aggregate-ethernet <*lag_name*> **storm-control broadcast pps**

Parameter
• <*lag_name*> Name of LAG interface.
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Packets per second, [0..30000000]

Example
• This example set broadcast storm control for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 storm-control broadcast pps 1000
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan

Users can add static mac address for a specific LAG.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **static-ethernet-switching mac-address** <*macaddr*> **vlan** <*vlan-id*>
delete interface aggregate-ethernet <*lag_name*> **static-ethernet-switching mac-address** <*macaddr*> **vlan** <*vlan-id*>

Parameter
• <*lag_name*> Name of LAG interface.
•<*macaddr*> static mac address.
•<*vlan-id*> vlan identifier, the range is between 1 to 4094.

Example
• This example is to configure mac-addr 12:11:11:11:11:11 for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 static-ethernet-switching mac-address 12:11:11:11:11:11 vlan 1
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> snmp-trap

Users can eable or disable snmp trap when necessary.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **snmp-trap** <*bool*>
delete interface aggregate-ethernet <*lag_name*> **snmp-trap**

Parameter
• <*lag_name*> Name of LAG interface.
•<*bool*> Snmp trap when port link up and down

- **true** enable snmp-trap
- **false** disable snmp-trap

Example
• This example enable snmp-trap for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 snmp-trap true
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> mtu

Users can set maximum transmit packet size for a specified LAG.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **mtu** <*value*>
delete interface aggregate-ethernet <*lag_name*> **mtu**

Parameter
• <*lag_name*> Name of LAG interface.
• <*value*> maximum transmit packet size identifier(in octets),value is between 64 to 9216.

Example
• This example sets MTU to 1024 for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 mtu 1024
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> hash-mapping mode

This command is to control the data packets to forward on a specified LAG .

> NOTE :
>
> The configuration of this command takes effect only on known unicast traffic.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **hash-mapping mode** *<mode>*
delete interface aggregate-ethernet *<lag_name>* **hash-mapping mode**

Parameter
• *<lag_name>* Name of LAG interface.
•*<mode>* Configure hash mapping mode. The default value is **ethernet-source-destination**.

- **advance** Use global advanced configure as hash-key
- **advanced-resilient** Use resilient hashing with advanced configure as key
- **ethernet-destination-only** Use destination mac as hash-key
- **ethernet-source-destination** Use source and destination mac as hash-key
- **ethernet-source-only** Use source mac as hash-key
- **ip-destination-only** Use destination ip as hash-key
- **ip-source-destination** Use source and destination ip as hash-key
- **ip-source-only** Use source ip as hash-key

Example
• This example is configure hash mapping mode to ethernet-destination-only advance for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 hash-mapping mode ethernet-destination-only
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id

The native VLANID is the ID of the default VLAN (usually vlan 1) in which the port belonged to. User can change the native VLANID for port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching native-vlan-id** <*vlan-id*>
delete interface aggregate-ethernet <*lag_name*> f**amily ethernet-switching native-vlan-id** <*vlan-id*>

Parameter
• <*lag*> Name of LAG interface.
• <*vlan_id*> The native-vlan-id ,VLAN identifier to associate with untagged packets .The valid VLAN number range is 1-4094.

Example
• This example creates VLAN 3 and puts ae1 on this VLAN:

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 3
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode

Users can configure a Q-in-Q tunnel mode for a logical port. By default, the mode is none.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling mode** *<mode>*

Parameter
• *<lag_name>* Name of LAG interface.
• *[mode]* Q-in-Q tunnel mode.

- external: customer mode
- internal: service provider mode
- none: Disable tunneling mode,default mode

Example
• This example is to set Q-in-Q tunnel mode for ae1 port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress

Users can configure/delete a Q-in-Q tunnel for inbound traffic on a logical port.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling ingress** *<text>*
delete interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling ingress** *<text>*

Parameter
• *<lag_name>* Name of LAG interface.
• *<text>*Tunneling for entering traffic

Example
• This example is to configure a Q-in-Q tunnel for inbound traffic on ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type

Set or delete an EtherType value on Q-in-Q tunnel for a logical port.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling ether-type** *<value>*

To delete enter:
delete interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling ether-type** *<value>*

Parameter
<lag_name> Name of LAG interface.
<value> EtherType value:

- **0x8100**
- **0x88a8**
- **0x9100**
- **0x9200**

Example
This example is to select a Ethertype value on Q-in-Q tunnel for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling ether-type 0x8100
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress

Configure or delete a Q-in-Q tunnel for outband traffic on a LAG.

Command Syntax
set interface aggregate-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling egress** *<text>*

To delete the configuration enter:
delete interface gigabit-ethernet *<lag_name>* **family ethernet-switching dot1q-tunneling egress** *<text>*

Parameter
• *<lag_name>* Name of LAG interface.
• *<text>Q-in-Q t*unneling foroutband traffic.

Example
This example is to configure a Q-in-Q tunnel for egress logical port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling egress t2
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> crossflow local-control

Enable or disable local-control function of crossflow for a logical port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **crossflow local-control** <true | false**>**

To delete the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **crossflow local-control**

Parameter

- <*lag_name*> Name of LAG interface.
- true: enable local control, this is the default mode.
- false: disable local control

Example
The example disables local-control function of crossflow on port ae1.

```
admin@XorPlus# set aggregate-ethernet ae1 crossflow local-control false
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> crossflow enable

Enable or disable the crossflow mode in a logical port.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **crossflow enable** <true | false>

To delete the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **crossflow enable**

Parameter

- *<lag_name>* Name of LAG interface.
- true: enable crossflow
- false: disable crossflow

Example

This example enables crossflow in ae1 port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 crossflow enable true
admin@XorPlus#commit
```

interface aggregate-ethernet <lag_name> backup-port mode

User can set preemption mode of a logical port.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **backup-port mode** <bandwidth | forced | Off>

To return to the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **backup-port mode**

Parameter

- *<lag_name>* Name of LAG interface.
- bandwidth: higher bandwidth interface preferred
- forced: active interface preferred,the default mode
- Off: turn off preemption

Example

This example is to set the port preemption mode to bandwidth:

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port mode bandwidth
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> backup-port interface

User can configure two physical ports or two LAGs as Flex Links or one physical port and one LAG as Flex Links.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **backup-port interface** *<interface_number>*

To return the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **backup-port interface**

Parameter

- *<lag_name>* Name of a configured LAG interface.
- *<interface_number>* Set backup port of an interface, which will disable RSTP/MSTP.

Example

This example is to set Flex links between a physical port and a LAG :

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port interface ge-1/1/3
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> backup-port delay

Set backup port delay time, in seconds, to a port.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **backup-port delay** *<seconds>*

To return the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **backup-port delay**

Parameter

- *<lag_name>* Name of a configured LAG interface.
- *<seconds>* Preemption delay, in seconds (range: 0 through 300 seconds)

Example

This example is to set the delay time to 20 seconds:

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port delay 20
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port

Configure min-selected-port for a specified logical port (LAG). Min-selected-port denotes that the LAG is up only when no fewer than the defined number of ports are up.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **aggregated-ether-options min-selected-port** *<port-id>*

To return to the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **aggregated-ether-options min-selected-port**

Parameter

<lag_name>: Specifies a configured LAG interface name.
<port-id>: Minimum number of selected ports (range: **1** through **8**)

Example

This example is to configure min-selected-port for ae1.

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options min-selected-port 1
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control

Configure flow-control for a logical port.

> On N1148T-ON platform, flow control in the inbound direction of the interface is not supported.

Command Syntax

set interface aggregate-ethernet *<lag_name>* **aggregated-ether-options flow-control** <true | false>

To return the configuration enter:
delete interface aggregate-ethernet *<lag_name>* **aggregated-ether-options flow-control**

Parameter

- *<lag_name>*--Enter the name of the configured LAG interface.
- true: enable flow control
- false: disable flow control

Example

This example enables flow-control on the LAG ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options flow-control true
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field vlan disable

Use this command to enables aggregate load balancing hash map on the VLAN.

Command Syntax

set interface aggregate-balancing hash-mapping field vlan disable <true | false>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field vlan disable

Parameter

- **true**--disable vlan
- **false**--enable vlan

Example

This example is to enable ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field vlan disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field port-source disable

This command designates data packets to be forwarded via the port-source.

Command Syntax

set interface aggregate-balancing hash-mapping field port-source disable <true | false>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field port-source disable

Parameter

- **true**--disable port-source
- **false**--enable port-source

Example

This example enables data packets to be forwarded via ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field port-source disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field port-destination disable

This command designates data packets to be forwarded via the port-destination.

Command Syntax

set interface aggregate-balancing hash-mapping field port-destination disable <**true** | **false**>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field port-destination disable

Parameter

- **true**--disable port-destination
- **false**--enable port-destination

Example

This example enables data packets to be forwarded via port-destination:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field port-destination disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-source disable

This command designates data packets to be forwarded via the IP source.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-source disable <**true** | **false**>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-source disable

Parameter

- **true**--disable ip-source
- **false**--enable ip-source

Example

This example enables forwarding of data packets via ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-source disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-protocol disable

This command designates data packets to be forwarded via the IP protocol.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-protocol disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-protocol disable

Parameter

- **true**--disable ip-protocol
- **false**--enable ip-protocol

Example

This example enables forwarding of data packets via the ip-protocol:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-protocol disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-destination disable

This command designates data packets to be forwarded via ip-destination.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-destination disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-destination disable

Parameter

- **true**--disable ip-destination
- **false**--enable ip-destination

Example

This example enables data packet fowarded by ip-destination:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-destination disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ingress-interface disable

This command designates data packets to be forwarded via the ingress-interface.

Command Syntax

set interface aggregate-balancing hash-mapping field ingress-interface disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ingress-interface disable

Parameter

- **true--**disable ingress-interface
- **false--**enable ingress-interface

Example

This example enables ingress-interface:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ingress-interface disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-type disable

This command designates data packets to be forwarded via the ethernet-type.

Command Syntax

set interface aggregate-balancing hash-mapping field ethernet-type disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-type disable

Parameter

- **true**--disable ethernet-type
- **false**--enable ethernet-type

Example

This example enables data packets to be forwarded via ethernet-type:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-type disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-source-address disable

This command designates data packets to be forwarded via ethernet-source-address.

Command Syntax

set interface aggregate-balancing hash-mapping field ethernet-source-address disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-source-address disable

Parameter

- **true**--disable ethernet-source-address
- **false**--enable ethernet-source-address

Example

This example enables data packets to be forwarded via ethernet-source-address:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-source-address disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-destination-address disable

This command designates data packets to be forwarded via the ethernet-destination-address.

Command Syntax

Set interface aggregate-balancing hash-mapping field ethernet-destination-address disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-destination-address disable

Parameter

- **true**--disable ethernet-destination-address
- **false**--enable ethernet-destination-address

Example

This example enables data packets forwarded by ethernet-destination-address:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-destination-address disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping randomized-load-balancing

The **set interface ecmp hash-mapping randomized-load-balancing** command enables Randomized Load Balancing of ECMP (Equal-Cost Multi-Path Routing). That is to say, the next hop of the message is randomly generated among multiple equivalent routes.

The **delete interface ecmp hash-mapping randomized-load-balancing** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping randomized-load-balancing

delete interface ecmp hash-mapping randomized-load-balancing

Parameter

Null.

Example

- Enable Randomized Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping randomized-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping round-robin-load-balancing

The **set interface ecmp hash-mapping round-robin-load-balancing** command enables round robin mode of ECMP (Equal-Cost Multi-Path Routing) load balancing. That is, each equivalent route to the same destination address alternately forwards the traffic. For known unicast, if the packets have approximately the same length, you can choose to configure round-robin-based per-packet load balancing to achieve traffic load balancing.

The **delete interface ecmp hash-mapping round-robin-load-balancing** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping round-robin-load-balancing

delete interface ecmp hash-mapping round-robin-load-balancing

Parameter

Null.

Example

- Enable round robin mode of ECMP load balancing.

```
admin@PICOS# set interface ecmp hash-mapping round-robin-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping resilient-load-balancing

The **set interface ecmp hash-mapping resilient-load-balancing** command enables resilient load balancing of ECMP (Equal-Cost Multi-Path Routing).

The **delete interface ecmp hash-mapping resilient-load-balancing** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping resilient-load-balancing

delete interface ecmp hash-mapping resilient-load-balancing

Parameter

Null.

Usage Guidelines

Resilient Hashing is an advanced load-balancing mechanism used in ECMP routing to ensure stable traffic distribution even when network topology changes occur (e.g., link failures or additions). It minimizes flow remapping, reducing disruptions and preserving packet ordering.

Traditional ECMP hashing distributes flows based on a hash function applied to fields such as *source/destination IPs*, *ports*, and *protocols*. However, when a path fails or a new path is added, standard ECMP can rehash all flows, leading to disruptions. Resilient Hashing aims to minimize this rehashing effect by maintaining as many existing flow-to-path mappings as possible.

1. **Handling Path Failures**

- When an ECMP path fails, only the affected flows are remapped to the remaining available paths.
- Traditional ECMP would recompute all flows, potentially shifting a large portion of traffic, while resilient hashing limits the impact.

2. **New Path Additions**

- If a new ECMP path is introduced, it is added gradually rather than forcing a full redistribution of flows.
- This prevents packet reordering and reduces the risk of microbursts.

Example

- Enable Resilient Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping resilient-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping dlb-normal

The **set interface ecmp hash-mapping dlb-normal** command enables normal mode of Dynamic Load Balancing for ECMP (Equal-Cost Multi-Path Routing).

The **delete interface ecmp hash-mapping dlb-normal** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping dlb-normal [**flowset-time** <*flowset-time*>]

delete interface ecmp hash-mapping dlb-normal

Parameter

Parameter	Description
flowset-time <*flowset-time*>	Optional. Specifies the inactive time interval for the flows. The value is an integer ranging from 16 to 32767 microseconds. The default value is 512 microseconds.

Usage Guidelines

After enabling the dynamic load sharing function, the traffic of Equal-Cost Multi-Path Routing (ECMP) can be distributed to different member links through dynamic load sharing, ensuring load balancing between member links.

Example

- Enable normal mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping symmetric

The **set interface ecmp hash-mapping symmetric** command enables Symmetric Hash for ECMP (Equal-Cost Multi-Path Routing) load balancing.

The **delete interface ecmp hash-mapping symmetric** command deletes the configuration.

- Make sure that the settings for the source IP and destination IP fields match, and that the settings for the source port and destination port fields match; otherwise symmetric hashing is disabled automatically.
- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping symmetric <**true** | **false**>

delete interface ecmp hash-mapping symmetric

Parameter

Null.

Parameter	Description
<**true** | **false**>	Enables or disables Symmetric Hash for ECMP. The value could be **true** or **false**. • **true**: Enables Symmetric Hash for ECMP. • **false**: Disables Symmetric Hash for ECMP. The default value is **false**.

Example

- Enable Symmetric Hash for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping symmetric true
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping dlb-optimal

The **set interface ecmp hash-mapping dlb-optimal** command enables optimal mode of Dynamic Load Balancing for ECMP (Equal-Cost Multi-Path Routing).

The **delete interface ecmp hash-mapping dlb-optimal** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**rround-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping dlb-optimal

delete interface ecmp hash-mapping dlb-optimal

Parameter

None.

Usage Guidelines

The Optimal mode of dynamic load balancing uses a per-packet distribution mechanism, where the device forwards packets to the link with the lighter load based on the real-time load status of each link. In this mechanism, if two consecutively forwarded packets belong to the same flow and the time interval between them is shorter than the maximum transmission delay among the links, and the device chooses different forwarding links for these two packets, out-of-order packets may occur on the receiving end.

Example

- Enable optimal mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-optimal
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping dlb-assigned

The **set interface ecmp hash-mapping dlb-assigned** command enables assigned mode of Dynamic Load Balancing for ECMP (Equal-Cost Multi-Path Routing).

The **delete interface ecmp hash-mapping dlb-assigned** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system restart is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric, resilient-load-balancing, dlb-normal**, **dlb-optimal** and **dlb-assigned**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping dlb-assigned

delete interface ecmp hash-mapping dlb-assigned

Parameter

None.

Usage Guidelines

In Assigned mode dynamic load balancing, the packet to be forwarded follows the same path as the previous packet in its flow. If the packet is the first one in its flow, a member link is selected for forwarding based on the hash result using a static load balancing mechanism.

Example

- Enable assigned mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-assigned
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface gigabit-ethernet breakout

The **set interface gigabit-ethernet breakout** command breaks out the 40GE, 100GE, 200GE and 400GE interfaces into four split interfaces. The 40GE interface is split into four 10GE interfaces; the 100GE interface is split into four 25GE interfaces; the 200GE interface is split into four 50GE interfaces; the 400GE interface is split into four 100GE interfaces.

NOTEs:

- Restart PICOS after committing this command to make the setting take effect.
- For 400GE and 200GE interfaces, after executing this command, you can furtherly configure the breakout type through command **set interface gigabit-ethernet breakout-type**. For details, see Configuring set interface gigabit-ethernet breakout-type.
- When performing the port breakout and merge operation, before restarting the system, you need to manually delete the configurations of the unavailable interfaces, to make sure that the configuration file can be loaded normally when the system boots up.
- From PICOS 3.7.3.4, AS7726_32X supports splitting a 100G port into 2x50G or 4x25G or 4x10G ports using command **set interface gigabit-ethernet** <*port-name*> **breakout true** and **set interface gigabit-ethernet breakmap** under L2/L3 mode.

Command Syntax

set interface gigabit-ethernet <*port-name*> **breakout** <**true | false**>

Parameter

Parameter	Description
gigabit-ethernet <*port-name*>	Specifies the port name of 40G, 100G, 200G or 400G port.
breakout <true | false>	Specifies the breakout mode. The value could be **true** or **false**. • **true**: breakout the specified port. • **false**: merge the specified port.

Usage Guidelines

The 40GE interfaces can be split into 4 x 10GE interfaces, the 100GE interface can be split into 4 x 25G or 4 x 10G Ethernet interfaces. By default, the 100G interface is split into 4 x 25G Ethernet interfaces. If you want to split into 4 x 10G Ethernet interfaces, you need to configure the four interfaces rate to 10G through the command line after port breakout. Note: The rate of the four interfaces is required to be consistent.

The 200GE interfaces can be split into 4 x 50GE, 4 x 25GE, 2 x 100GE or 2×50GE interfaces. By default, the 200GE interface is split into 4 x 50GE interfaces. To split into 4 x 25G or 2×50GE Ethernet interfaces, insert the 100GE optical module and execute the **set interface gigabit-ethernet breakout-type** command; to split into 2 x 100G Ethernet interfaces, insert the 200GE optical module, and execute the **set interface gigabit-ethernet breakout-type** command.

The 400GE interfaces can be split into 4 x 100GE or 2 x 200GE interfaces. By default, the 400GE interface is split into 4 x 100GE interfaces. To split into 2 x 200G Ethernet interfaces, execute the **set interface gigabit-ethernet breakout-type** command.

After a single interface is split into four interfaces, the 10GE split optical interface or the 25GE split optical interface supports the same configurations and features as other non-breakout optical interface except that the interface is named in a different way. For example, the port name of the 100GE and 40GE optical interfaces is xe-1/1/n before port breakout; however, after port breakout the port names of the four interfaces are xe-1/1/n.1, xe-1/1/n.2, xe-1/1 /n.3 and xe- 1/1/n.4.

Example

- Split the 40GE port xe-1/1/25 into 4 x 10GE ports.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/25 breakout true
admin@XorPlus# commit
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading startup configuration will fail.
admin@XorPlus# exit
admin@XorPlus> request system reboot
```

- Do not split the 100G port xe-1/1/53.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/53 breakout false
admin@XorPlus# commit
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading startup configuration will fail.
admin@XorPlus# exit
admin@XorPlus> request system reboot
```

set interface gigabit-ethernet cdr

The **set interface gigabit-ethernet cdr** command configures whether to enable or disable the CDR function.

NOTEs:

- CDR function can only be configured on the 800G, 400G, 200G, 100G or 40G optical module interface and the split interfaces broke out from them.
- The CDR configurations of split interfaces which broke out from the 800G, 400G, 200G, 100G or 40G optical module interface should be the same.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **cdr** [**true | false**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface or split interface name. For example, te-1/1/49 and xe-1/1/49.1.
cdr [**true	false**]	Configures whether to enable or disable the CDR function. The value is **true** or **false**. **true**: enables the CDR function. **false**: disables the CDR function. The default value is **true**.

Example

- Enable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr true
admin@Xorplus# commit
```

- Disable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr false
admin@Xorplus# commit
```

VLAN Configuration Commands

This section contains descriptions of the CLI commands that this chapter references.

- set vlans dot1q-tunneling egress from
- set vlans dot1q-tunneling egress then action
- set vlans dot1q-tunneling egress then service-vlan
- set vlans dot1q-tunneling ingress from double-tag service-vlan
- set vlans dot1q-tunneling ingress from one-tag customer-vlan-list
- set vlans dot1q-tunneling ingress from untag enabled
- set vlans dot1q-tunneling ingress then
- set vlans vlan-id
- set vlans vlan-id description
- set vlans vlan-id l3-interface
- set vlans vlan-id vlan-name
- set vlans vlan-id private-vlan mode
- set vlans vlan-id private-vlan association
- set mac-map mac-address vlan
- run show vlans
- run show vlans private-vlan
- run show vlans private-vlan type
- run show mac-map
- set tracemac disable
- tracemac

set vlans dot1q-tunneling egress from

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress from** command in L2/L3 configuration mode. If the customer VLAN or service VLAN tag frame is specified, it can pass through the port.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **from** { **customer-vlan** | **service-vlan** } *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
customer-vlan	The customer VLAN identifier.
service-vlan	The service VLAN identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

This example configures tunneling *T0*, such that if the customer tag frame is 10 and the service tag frame is 100, the packet can pass through the port:

```
admin@Switch# set vlans dot1q-tunneling egress T0 from customer-vlan 10
admin@Switch# set vlans dot1q-tunneling egress T0 from service-vlan 100
```

set vlans dot1q-tunneling egress then action

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress then action** command in L2/L3 configuration mode. If a packet can pass through the port, it needs to be modified by the action.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **then action** { **change** | **none** | **one** | **two** }

Parameters

tunnel-id	Tunnel identifier.
change	Change the service VLAN tag.
none	Strip both the customer and service VLAN tags.
one	Retain the customer VLAN tag.
two	Retain both the customer and service VLAN tag.

Examples

This example explains how to configure the tunneling t5. If the packet can pass the port, the packet does not need to be changed.

- The service and customer tag frame of the packet need not to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action none
```

- The outside service tag frame of the packet need to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action one
```

- The service and customer tag frame of the packet need to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action two
```

- The service tag frame of the packet need to be replaced by 200

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action change
admin@XorPlus# set vlans dot1q-tunneling egress t5 then service-vlan 200
admin@XorPlus# commit
```

set vlans dot1q-tunneling egress then service-vlan

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress then service-vlan** command in L2/L3 configuration mode. If a packet passes through the port, the service tag of the packet needs to be changed.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **then service-vlan** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier.

Examples

The following example shows how to configure *T0* tunneling. If a packet wants to pass through the port, the service tag of the packet needs to be replaced by 300:

```
admin@Switch# set vlans dot1q-tunneling egress T0 then service-vlan 300
```

set vlans dot1q-tunneling ingress from double-tag service-vlan

To configure tunneling for ingress traffic at a port, use the **set vlans dot1q-tunneling ingress from double-tag service-vlan** command in L2/L3 configuration mode. If a packet has double tags and service vlan is specified, the packet can pass through the port.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from double-tag service-vlan** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

The following example configures T0 tunneling for ingress traffic. If the packet has double tags and service vlan is 100, it can pass through the port:

```
admin@Switch# set vlans dot1q-tunneling ingress T0 from double-tag service-vlan 100
```

set vlans dot1q-tunneling ingress from one-tag customer-vlan-list

To configure tunneling for ingress traffic at a port, use the **set vlans dot1q-tunneling ingress from one-tag customer-vlan-list** command in L2/L3 configuration mode. If the packet has a single tag and customer VLAN is specified, it can pass through the port.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from one-tag customer-vlan-list** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier.

Examples

The following example configures the tunneling *T1* for ingress traffic. If the packet has a single tag and customer VLAN is 10, it can pass through the port.

```
admin@Switch# set vlans dot1q-tunneling ingress T1 from one-tag customer-vlan-list 10
```

set vlans dot1q-tunneling ingress from untag enabled

To configure tunneling for untagged ingress traffic use the **set vlans dot1q-tunneling ingress from untag enabled** command in L2/L3 configuration mode.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from untag enabled** { **true** | **false** }

Parameters

tunnel-id	Tunnel identifier.
true	Enable matching untagged traffic.
false	Disable matching untagged traffic.

Examples

The following configuration checks if untagged frames are received by the port or not:

```
admin@Switch# set vlans dot1q-tunneling ingress T1 from untag enabled true
admin@Switch# set vlans dot1q-tunneling ingress T1 from untag enabled false
```

set vlans dot1q-tunneling ingress then

To configure tunneling for ingress traffic received at a port and adding customer or service tag to frames, use the **set vlans dot1q-tunneling ingress then** command in L2/L3 configuration mode.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **then** { **customer-vlan** | **service-vlan** } *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
customer-vlan	The new customer VLAN identifier.
service-vlan	The new service VLAN identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

The following example configures the T0 tunneling to add customer tag 10 and service tag 100 to frames:

```
admin@Switch# set vlans dot1q-tunneling ingress T0 then customer-vlan 10
admin@Switch# set vlans dot1q-tunneling ingress T0 then service-vlan 100
```

set vlans vlan-id

The command set vlans vlan-id can be used to create a VLAN. Vlan-id 1 exists by default.

> **NOTE:**
> VLAN IDs (VLAN 1-4094) have been pre-configured in the system from version 4.3.2 and are not user-deletable. Users no longer need to use command **set vlans vlan-id** <*vlan-id*> to create VLAN IDs.

Command Syntax
set vlans vlan-id <*vlan-id*>
delete vlans vlan-id <*vlan-id*>

Parameter
• <*vlan_id*> VLAN tag identifier. The valid VLAN numbers range 1-4094. User can specify a range of VLAN numbers, e.g. 2,3,5-100.

Example
• This example creates VLAN 10:

```
admin@XorPlus# set vlans vlan-id 10
admin@XorPlus# commit
```

set vlans vlan-id description

To add description for a VLAN, use the **set vlans vlan-id description** command in L2/L3 configuration mode.

Command Syntax

set vlans vlan-id *vlan-id* **description** *description*
delete vlans vlan-id *vlan-id* **description**

Parameters

vlan-id	VLAN identifier. The range of values is from 1 to 4094. A range of VLAN identifiers can be specified, for example, 2,3,5-100.
description	VLAN description in free text format.

Example

The following example creates description for VLAN 10:

```
admin@Switch# set vlans vlan-id 10 description "My Favorite VLAN"
```

set vlans vlan-id l3-interface

To associate a Layer 3 interface with a VLAN, use the **set vlans vlan-id l3-interface** command. To remove the Layer 3 interface, use the **delete** form of the command.

Command Syntax

set vlans vlan-id *vlan-id* **l3-interface** *interface-name*
delete vlans vlan-id *vlan-id* **l3-interface**

Parameters

vlan-id	VLAN identifier. The range of allowed VLAN identifiers is 1-4094. A range of VLAN identifiers can be used, for example, 2,3,4,5-100.
interface-name	Name of the Layer 3 interface.

Example

- This example associates a Layer 3 interface vlan-1 with VLAN 10 and then removes the Layer 3 interface from the VLAN:

```
admin@Switch# set vlans vlan-id 10 l3-interface vlan-1
admin@Switch# commit
admin@Switch# delete vlans vlan-id 10 l3-interface
admin@Switch# commit
```

set vlans vlan-id vlan-name

To create a VLAN, use the **set vlans vlan-id** command in L2/L3 configuration mode. To give a name to the VLAN, use the optional **vlan-name** keyword. To remove a VLAN, use the **delete** form of the command.

Command Syntax

set vlans vlan-id *vlan-id* [**vlan-name** *vlan-name*]
delete vlans vlan-id *vlan-id*

Parameters

vlan-id	VLAN identifier. The range is from 1 to 4094. A range of VLAN identifiers can be specified, for example, 2,3,5-100.
vlan-name	VLAN name. Up to 32 alphanumeric characters in length.

Example

This example creates VLAN 10 and names it MyVLAN:

```
admin@Switch# set vlans vlan-id 10 vlan-name MyVLAN
```

set vlans vlan-id private-vlan mode

The **set vlans vlan-id private-vlan mode** command configures the PVLAN mode of a VLAN.

Command Syntax

set vlans vlan-id <*vlan-id*> **private-vlan mode** <**primary** | **community** | **isolated**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
private-vlan mode <**primary**	**community**	**isolated**>	Specifies the PVLAN mode of a VLAN. The value could be **primary**, **community** or **isolated**. • **primary**: Configures a VLAN as a primary VLAN. • **community**: Configures a VLAN as a community VLAN. • **isolated**: Configures a VLAN as an isolated VLAN.

Usage Guidelines

PVLAN function involves the following VLAN types:

- Primary VLAN: allows member interfaces to communicate with each other and with interfaces in secondary VLANs.
- Secondary VLAN
- Isolated VLAN: allows member interfaces to communicate with only interfaces in the primary VLAN. An interface in an isolated VLAN cannot communicate with interfaces in the same VLAN or other secondary VLANs.
- Community VLAN: allows member interfaces to communicate with each other within the same VLAN and interfaces in the primary VLAN. An interface in a secondary VLAN cannot communicate with interfaces in other secondary VLANs.

NOTE:

If you want to change a private VLAN to a normal VLAN, you need to remove the configurations for PVLAN-related binding relationship before you can remove the PVLAN mode configuration. For example, if you use the **set vlans vlan-id** <*vlan-id*> **private-vlan association** <*secondary-vlan-list*> command for PVLAN association, remove the binding relationship first before you can change the private VLAN to a normal VLAN.

Similarly, it also requires to remove the private VLAN relevant configuration before changing the role of a private VLAN to another PVLAN type, e.g. when changing the PVLAN type from primary VLAN to secondary VLAN.

Example

- Configure a primary VLAN.

```
admin@Xorplus# set vlans vlan-id 2 private-vlan mode primary
admin@Xorplus# commit
```

set vlans vlan-id private-vlan association

The **set vlans vlan-id private-vlan association** command associates the secondary VLAN list with the primary VLAN.

Command Syntax

set vlans vlan-id <*vlan-id*> **private-vlan association** <*secondary-vlan-list*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies the primary VLAN ID. The value is an integer.
<*secondary-vlan-list*>	Specifies secondary VLAN list in a primary VLAN. The value is a string. E.g. 3, 5, 100-200. The VLANs in the list need to be previously configured as either an isolated VLAN or a community VLAN.

Usage Guidelines

Configure the association between primary VLAN and secondary VLAN list to specify a PVLAN pair.

NOTE:

- Before setting this command, use command set vlans vlan-id <*vlan-id*> private-vlan mode <primary | community | isolated> to configure the PLAN types.
- A primary VLAN can be associated with multiple community VLANs and only one isolated VLAN.
- A secondary VLAN (isolated or community) can be associated with only one primary VLAN.
- If you run this command with the same primary VLAN multiple times, only the latest configuration takes effect.
- Before modifying or deleting PVLAN association configuration, you need to delete all the PVLAN settings of the involved Private VLANs.

Example

- Associate the secondary VLAN list 2-3 with the primary VLAN 5.

```
admin@Xorplus# set vlans vlan-id 5 private-vlan association 2-3
admin@Xorplus# commit
```

set mac-map mac-address vlan

The **set mac-map mac-address vlan** command configures MAC address and VLAN mapping entry.

The **delete mac-map mac-address vlan** command deletes the configuration.

> **NOTE:**
> The same MAC address can be bound to no more than one VLAN.

Command Syntax

set mac-map mac-address <*mac-address*> **vlan** <*vlan-id*>

Parameters

Parameter	Description
mac-address <*mac-address*>	Specifies a MAC address binding to the VLAN. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. MAC address cannot be set to all-0, all-F or multicast address.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1-4094.

Example

- Configure MAC address 00:22:22:22:22:20 to VLAN 200 mapping entry.

```
admin@Xorplus# set mac-map mac-address 00:22:22:22:22:20 vlan 200
admin@Xorplus# commit
```

run show vlans

The **run show vlans** command displays information about VLANs configured on a switch. With the command display VLANID, Tag, and Interface by default, user can display the brief, detail or special VLANID information.

Command Syntax

run show vlans <*text*>

Parameter

• <*text*> The specific information, options include:

- **brief** Show vlan brief information
- **detail** Show vlan detail information
- **vlan-id** <*vlan-id*> Show specific vlan detail information

Example

• This example shows VLAN 10:

```
admin@XorPlus# run show vlans
VlanID Vlan Name  Tag      Interfaces
------ --------   -------- ------------------------------------------------------
1      default    untagged ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5, ge-1/1/6
                           ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10, ge-1/1/11
                           ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15, ge-1/1/16
                           ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20, ge-1/1/21
                           ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25, ge-1/1/26
                           ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30, ge-1/1/31
                  tagged
10     aaa        untagged ge-1/1/1
                  tagged

admin@XorPlus# run show vlans vlan-id 10
VLAN ID: 10
VLAN Name: aaa
Description: myvlan
vlan-interface:
Routed-interface:
Number of member ports: 1
Untagged port: 1
Tagged port: None
```

run show vlans private-vlan

The **run show vlans private-vlan** command shows the PVLAN configuration information.

Command Syntax

run show vlans private-vlan

Parameter

Null.

Example

- View the PVLAN configuration information.

```
admin@Xorplus# run show vlans private-vlan
Primary   Secondary  Type            Tag         Interfaces
-------   ---------  -----------     --------    --------------------------
5                    primary         untagged    te-1/1/1
                                       tagged
          2          isolated        untagged    ge-1/1/1, ge-1/1/2
                                       tagged
          3          community       untagged    ge-1/1/3, ge-1/1/4
                                       tagged
```

The field “**Tag**” indicates whether the packets will be tagged or not when they are sent from this port.

run show vlans private-vlan type

The **run show vlans private-vlan type** command is used to view the PVLAN type information.

Command Syntax

run show vlans private-vlan type

Parameter

Null.

Example

- View the PVLAN type information.

```
admin@Xorplus# run show vlans private-vlan type
Vlan Type
---- -----------
5    primary
2    isolated
3    community
```

run show mac-map

The **run show mac-map** command is used to view the configuration information of MAC-based VLAN.

Command Syntax

run show mac-map [**mac-address** <*mac-address*>]

Parameter

Parameter	Description
mac-address <*mac-address*>	Optional. Specifies a MAC address binding to the VLAN. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Example

- View the configuration information of MAC-based VLAN.

```
admin@Xorplus# run show mac-map
Total entries: 4096
MAC                VLAN
00:33:33:33:33:20  400
00:22:22:22:22:20  300

admin@Xorplus# run show mac-map mac-address 00:22:22:22:22:20
MAC                VLAN
00:22:22:22:22:20  300
```

set tracemac disable

The **set tracemac disable** command can be used to enable or disable MAC trace function.

The **delete tracemac disable** command deletes the configuration.

Command Syntax

set tracemac disable <**true | false**>

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable MAC trace function. The value could be **true** or **false**. • **true**: Disable MAC trace function. • **false**: Enable MAC trace function. By default, MAC trace function is disabled.

Example

- Enable MAC trace function.

```
admin@PICOS# set tracemac disable false
admin@PICOS# commit
```

tracemac

The **tracemac** command output shows the Layer 2 path connectivity between the current device and the destination device.

Command Syntax

run tracemac destination <*mac-address*> **vlan** <*vlan-id*>

Parameters

Parameter	Description
destination <*mac-address*>	Specifies a MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. MAC address cannot be set to all-0, all-F or multicast address.
vlan <*vlan-id*>	Specifies the VLAN ID of the destination MAC. The value is an integer that ranges from 1-4094.

Example

- Trace MAC destination device with MAC address 20:11:11:11:11:11:11 and belonging to VLAN 100.

```
admin@PICOS# run tracemac destination 22:11:11:11:11:11 vlan 4094
Hop   Hostname    Ingress port   Ingress mac        Egress port   Egress mac
----- ----------- -------------- ------------       ------------  ------------
1     PICOS       xe-1/1/1.1     70:72:cf:b7:65:45  te-1/1/5      70:72:cf:b7:65:45
2     PICOS       te-1/1/3       04:f8:f8:20:6c:7b  -             04:f8:f8:20:6c:7b
```

NOTE:

The ingress port and egress port in the output of the command only displays the member port of the LAG port.

Voice VLAN Configuration Commands

- set interface gigabit-ethernet voice-vlan mode
- set interface gigabit-ethernet voice-vlan tagged mode
- set interface gigabit-ethernet voice-vlan vlan-id
- set vlans voice-vlan aging
- set vlans voice-vlan dscp
- set vlans voice-vlan local-priority
- set vlans voice-vlan mac-address mask
- set vlans voice-vlan mac-address description
- show vlans voice-vlan
- show vlans voice-vlan oui
- show vlans voice-vlan vlan-id <text>

set interface gigabit-ethernet voice-vlan mode

The **set interface gigabit-ethernet voice-vlan mode** command configures the mode in which an interface is added to a voice VLAN.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan mode** <**auto** | **manual**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch.
mode <**auto**	**manual**>	Specifies the mode in which an interface is added to a voice VLAN.The value is **auto** or **manual**. • **auto**: indicates the automatic mode. • **manual**: indicates the manual mode. The default value is **auto**.

Usage Guidelines

Auto and manual mode determine the mode of the port when added to the voice VLAN.

- **Auto Mode**

In automatic mode, the system uses the protocol packets sent by the IP phone. If the source MAC address of the packets matches the OUI address, the system will automatically add the ingress port of the voice packet to the voice VLAN, and then install the ACL rules of voice VLAN and implement the priority of the packet. If the source MAC address of the packets matches no OUI address, the system will learn the source MAC address of the LLDP, LLDP-MED or CDP packet as the learned OUI and add the port to the voice VLAN.

You can set the voice VLAN aging time on the device. During the aging time, if no voice packet is received from the ingress port, the system deletes the port from the voice VLAN. The process of adding/deleting a port to the voice VLAN is implemented automatically by the system.

- **Manual Mode**

In manual mode, the port is added to voice VLAN manually. This type of port is not affected by the aging time of the voice VLAN. When the aging time expires, it is not deleted from the voice VLAN.

In manual mode, the ports is added to voice VLAN by manual configuration. If the source MAC address of the packets matches the OUI address, the system will install the ACL rules of voice VLAN and implement the priority of the packet. The process of adding/deleting a port to the voice VLAN is implemented manually by the administrator.

Example

- Configure interface ge-1/1/1 be added to the voice VLAN in auto mode.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan mode auto
admin@Xorplus# commit
```

set interface gigabit-ethernet voice-vlan tagged mode

The **set interface gigabit-ethernet voice-vlan tagged mode** command configures the tagged mode for the outgoing packet of a voice VLAN interface.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan tagged mode** <**tag | untag | auto**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch.
tagged mode <tag | untag | auto>	Configure the tagged mode for the outgoing packet of a voice VLAN interface. The value could be **tag**, **untag** or **auto**. • **tag**: the outgoing packets of a voice VLAN interface be tagged with the voice VLAN ID regardless of the protocol type used between the switch and the IP phone. • **untag**: the outgoing packets of a voice VLAN interface be untagged regardless of the protocol type used between the switch and the IP phone. • **auto**: the system automatically determines whether the outgoing packet of a voice VLAN interface be tagged with the voice VLAN ID per the protocol type. The value **auto** is the default and recommended value.

Usage Guidelines

For tagged mode auto,

- If the packet matches the user defined OUI addresses or the OUI addresses learned from CDP and LLDP protocols, the outgoing packet from a voice VLAN interface will be untagged when the tagged mode is auto.
- If the packet matches the OUI addresses learned from LLDP-MED protocol, the outgoing packet of a voice VLAN interface will be tagged with the voice VLAN ID based on the result of the LLDP-MED protocol negotiation between the switch and the IP phone when the tagged mode is auto.
  - If the negotiation result of LLDP-MED protocol between the switch and the IP phone is SUCCESS, the outgoing packet of a voice VLAN interface will be tagged with the voice VLAN ID.
  - Else if the negotiation result of LLDP-MED protocol between the switch and the IP phone is FAILURE, the outgoing packet of a voice VLAN interface will be untagged.

Example

- Configure the outgoing packet of a voice VLAN interface ge-1/1/1 be tagged with the voice VLAN ID.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan tagged mode tag
admin@Xorplus# commit
```

set interface gigabit-ethernet voice-vlan vlan-id

The **set interface gigabit-ethernet voice-vlan vlan-id** command configures an interface into voice VLAN.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan vlan-id** <*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch to be added to voice VLAN.
vlan-id <*vlan-id*>	Specifies a voice VLAN ID.

Example

- Configure interface ge-1/1/1 into voice VLAN 10.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan vlan-id 10
admin@Xorplus# commit
```

set vlans voice-vlan aging

The **set vlans voice-vlan aging** command configures the aging time for voice VLAN.

Command Syntax

set vlans voice-vlan aging <*aging-time*>

Parameter

Parameter	Description
aging <*aging-time*>	Specifies the aging time for voice VLAN. The value is an integer, in minutes, that ranges from 5 to 43200. The default value is 1440.

Usage Guidelines

You can set the voice VLAN aging time on the device. Until the aging time expires, if no voice packet is received from the ingress port, the system deletes the port from the voice VLAN.

- For the OUI of dynamic learning, when a LLDP neighbor entry in the MAC address table has aged, the aging time of voice VLAN starts. LLDP neighbor entry aging time is the “Time To Live” value in the received LLDP packet.
- For static OUI, when a MAC entry in the MAC address table has aged, the aging time of voice VLAN starts. The status of voice VLAN switches from working to aging, if no voice packet corresponding to the OUI is received until the aging timer expires, the status of voice VLAN switches from aging to idle. After which the learned OUI is cleared and the port is removed from the voice VLAN.

NOTE:

The voice VLAN aging time works only on auto mode.

Example

- Configure the aging time for voice VLAN to 30 minutes.

```
admin@Xorplus# set vlans voice-vlan aging 30
admin@Xorplus# commit
```

set vlans voice-vlan dscp

The **set vlans voice-vlan dscp** command modifies the DSCP value for the voice VLAN.

Command Syntax

set vlans voice-vlan dscp <*dscp-value*>

Parameter

Parameter	Description
dscp <*dscp-value*>	Specifies the DSCP value for the voice VLAN. The value is an integer that ranges from 0 to 63.

Usage Guidelines

Differentiated Services Code Point (DSCP) value is used to provide Diff-Serv (Differentiated Service) node behavior for the specified application type as defined in IETF RFC 2474. This 6 bit field may contain one of 64 code point values (0 through 63). The six bits Type of Service (TOS) field in the IPv4 data packet header are used for DSCP.

Example

- Configure the DSCP value to 50 for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan dscp 50
admin@Xorplus# commit
```

set vlans voice-vlan local-priority

The **set vlans voice-vlan local-priority** command modifies the 802.1p priority for the voice VLAN.

Command Syntax

set vlans voice-vlan local-priority <*priority-value*>

Parameter

Parameter	Description
local-priority <*priority-value***>**	Specifies the 802.1p priority for the voice VLAN. The value is an integer that ranges from 0 to 7.

Usage Guidelines

802.1p priority is the value of the priority field in the VLAN frame in IEEE 802.1Q standard, which contains the layer 2 priority to be used for the specified application type. This 3 bit field could specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004.

This configuration not only changes the 802.1p priority value in the packet, but also changes egress queue of the packet.

Example

- Configure the 802.1p priority to 7 for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan local-priority 7
admin@Xorplus# commit
```

set vlans voice-vlan mac-address mask

The **set vlans voice-vlan mac-address mask** command configures the OUI address for the voice VLAN.

Command Syntax

set vlans voice-vlan mac-address <*mac-address***> mask** <*oui-mask*>

Parameter

Parameter	Description
mac-address <*mac-address***>**	Specifies the OUI address for voice VLAN. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The address cannot be all 0s, multicast address, or broadcast address.
mask <*oui-mask***>**	Specifies the mask for the OUI address.

Usage Guidelines

OUI refers to the first 24 bits (binary) of the MAC address that can be used to represent a MAC address segment, which is a globally unique identifier assigned by the IEEE to different device vendors, each device vendor then allocates 24 bit to form a 48-bit MAC address.

In voice VLAN, the OUI is not necessarily 24 bits long which depends on the mask value. The OUI is the result of the AND operation between the MAC address and the mask in the **set vlans voice-vlan mac-address mask** command.

The switch identifies packets as voice data when the source MAC address matches the system pre-configured Organizationally Unique Identifier (OUI).

> **NOTE:**
>
> The system supports a maximum of 10 OUIs, including the default 7 OUIs. In PICOS 2.11.4 and the later version , there is no default OUI, the user is allowed to configure a maximum of 10 OUIs.

Example

- Configure an OUI address for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan mac-address 00:11:11:00:00:01 mask ff:ff:ff:00:00:00
admin@Xorplus# commit
```

set vlans voice-vlan mac-address description

The **set vlans voice-vlan mac-address mask** command configures the description information for the OUI address.

Command Syntax

set vlans voice-vlan mac-address <*mac-address***> description** <*text*>

Parameter

Parameter	Description
mac-address <*mac-address***>**	Specifies the OUI address for voice VLAN. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The address cannot be all 0s, multicast address, or broadcast address.
description <*text***>**	Optional. Add the description information for the OUI address. The value is a string.

Example

- Configure the description information for the OUI address.

```
admin@Xorplus# set vlans voice-vlan mac-address 00:11:11:00:00:01 description CompanyPhone
admin@Xorplus# commit
```

show vlans voice-vlan

Show voice vlan detail information.

Command Syntax
show vlans voice-vlan

Description

Generally speaking, what the command shows contains two logical parts.

1.OUI

This part shows all the oui addresses and their mask and description.

```
Oui_Address          Mask                 Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0       Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0       Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0       Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0       Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0       Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0       Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0       3com phone
```

2.Specified voice-vlan id

The following example contains 4 voice-vlans. Let's take voice-vlan id:10 for example.

```
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86274sec
```

- Voice Vlan ID: 10 means the voice-vlan id is 10
- The following 3 items is global parameters, local priority, dscp and aging time is the same in all the 4 voice-vlans

```
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
```

- Port means the ports below are configured this voice-vlan id.
- Mode means voice-vlan mode of the port: auto or manual.
- Tagged means the outgoing packets with OUI source Mac-address from the port will be tagged of not. It has two values: true and false. True means tagged and false means untagged.
- Mac_address displays OUI source Mac-address the port has learned. It shows the result of Oui_Address AND mask.
- Status shows the voice-vlan working status of the port.

Status of Voice Vlan	Description
Aging:<text>sec	Only auto mode has this status. This port won't be in this vlan after <text> seconds.
Working	Voice vlan is working on the port. The port is in the vlan(voice-vlan id).
Idle	Only auto mode has this status, voice vlan is not working on the port.

Example
• This example is to show voice-vlan detail information, ge-1/1/1 is auto mode and aging, ge-1/1/2 is auto mode and working, ge-1/1/3 is auto mode but not working, ge-1/1/4 is manual mode

```
admin@XorPlus# run show vlans voice-vlan
Oui_Address          Mask                 Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0       Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0       Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0       Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0       Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0       Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0       Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0       3com phone
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86274sec
Voice Vlan ID:20
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
```

```
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------------
ge-1/1/2       auto      false     0:1:e3:0:0:0     Working
Voice Vlan ID:30
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------------
ge-1/1/3       auto      false                      Idle
Voice Vlan ID:40
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------------
ge-1/1/4       manual    false                      Working
```

show vlans voice-vlan oui

Show voice vlan oui detail information, including default oui, static oui and oui learned from LLDP packet.

Command Syntax
show vlans voice-vlan oui

Default OUI as below :

```
Oui_Address          Mask               Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0     Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0     Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0     Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0     Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0     Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0     Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0     3com phone
```

OUI Learned from LLDP packet as below :

```
LLDP_Oui_Address     Mask
22:22:22:22:22:33    ff:ff:ff:ff:ff:ff
22:22:22:22:22:44    ff:ff:ff:ff:ff:ff
```

> LLDP are deployed between pica8 switch and IP phone. This command can't show LLDP OUI address when switch doesn't receive any LLDP packet from IP phone.

Example

• This example is to show voice-vlan oui detail information::

```
admin@XorPlus# run show vlans voice-vlan oui
Oui_Address          Mask               Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0     Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0     Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0     Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0     Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0     Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0     Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0     3com phone
22:33:44:0:0:0       ff:ff:ff:0:0:0     user1

LLDP_Oui_Address     Mask
22:22:22:22:22:33    ff:ff:ff:ff:ff:ff
22:22:22:22:22:44    ff:ff:ff:ff:ff:ff
```

show vlans voice-vlan vlan-id <text>

Show special voice vlan id detail information.

Command Syntax
show vlans voice-vlan vlan-id <text>

Parameter
•<text> voice-vlan id, can't be the same with pvid or vlan-member

Example
• This example is to show voice-vlan detail information::

```
1.ge-1/1/1 is in suto mode and aging.
admin@XorPlus#  run show vlans voice-vlan vlan-id 10
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86143sec

2.ge-1/1/2 is in auto mode and working.
admin@XorPlus# run show vlans voice-vlan vlan-id 20
Voice Vlan ID:20
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/2       auto      false     0:1:e3:0:0:0     Working

3.ge-1/1/3 is in auto mode and not working.
admin@XorPlus# run show vlans voice-vlan vlan-id 30
Voice Vlan ID:30
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/3       auto      false                      Idle

4.ge-1/1/4 is in manual mode. It can't display any mac-addresses and status will always be working in this mode.
admin@XorPlus# run show vlans voice-vlan vlan-id 40
Voice Vlan ID:40
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/4       manual    false                      Working
```

Layer 3 Routing Commands

- run show neighbors
- run show route
- run show route forward-host
- run show route forward-route
- run show vrf
- set ip vrf
- set ip routing enable
- set system management-vrf enable
- BGP Commands
  - run show bgp
  - run show bgp neighbor
  - run show bgp route
  - run show bgp unicast neighbor graceful-restart
  - set protocols bgp aggregate-address
  - set protocols bgp always-compare-med
  - set protocols bgp bestpath as-path type multipath-relax
  - set protocols bgp bestpath bandwidth
  - set protocols bgp bestpath compare-routerid
  - set protocols bgp bestpath med missing-as-worst
  - set protocols bgp cluster-id
  - set protocols bgp graceful-shutdown
  - set protocols bgp listen
  - set protocols bgp local-as
  - set protocols bgp max-med
  - set protocols bgp multipath maximum-paths
  - set protocols bgp neighbor activate
  - set protocols bgp neighbor addpath-tx-all-paths
  - set protocols bgp neighbor addpath-tx-bestpath-per-as
  - set protocols bgp neighbor advertisement-interval
  - set protocols bgp neighbor allowas-in
  - set protocols bgp neighbor as-override
  - set protocols bgp neighbor capability extended-nexthop
  - set protocols bgp neighbor default-originate
  - set protocols bgp neighbor description
  - set protocols bgp neighbor disable-connected-check
  - set protocols bgp neighbor ebgp-multihop
  - set protocols bgp neighbor filter-list
  - set protocols bgp neighbor next-hop-self
  - set protocols bgp neighbor password
  - set protocols bgp neighbor peer-group
  - set protocols bgp neighbor prefix-list
  - set protocols bgp neighbor remote-as
  - set protocols bgp neighbor remove-private-as
  - set protocols bgp neighbor route-map
  - set protocols bgp neighbor route-reflector-client
  - set protocols bgp neighbor send-community
  - set protocols bgp neighbor shutdown
  - set protocols bgp neighbor soft-reconfiguration
  - set protocols bgp neighbor timers connect
  - set protocols bgp neighbor timers holdtime
  - set protocols bgp neighbor timers keepalive
  - set protocols bgp neighbor ttl-security hops
  - set protocols bgp neighbor update-source
  - set protocols bgp network
  - set protocols bgp network-import-check
  - set protocols bgp peer-group
  - set protocols bgp redistribute
  - set protocols bgp route-map delay-timer
  - set protocols bgp router-id
  - set protocols bgp table-map
  - set protocols bgp timers
  - set protocols bgp update-delay
  - set protocols bgp ebgp-requires-policy
  - set protocols bgp neighbor timers delayopen

- set protocols bgp neighbor maximum-prefix
- set protocols bgp neighbor maximum-prefix-out
- set protocols bgp neighbor port
- set protocols bgp neighbor sender-as-path-loop-detection
- set protocols bgp fast-external-failover
- set protocols bgp confederation identifier
- set protocols bgp confederation peers
- set protocols bgp dampening
- set protocols bgp default local-preference
- set protocols bgp as-notation
- set protocols bgp neighbor local-as

- OSPFv2 Commands
  - run clear ospf interface
  - run show ospf border-routers
  - run show ospf database
  - run show ospf interface
  - run show ospf neighbor
  - run show ospf route
  - run show ospf summary-address
  - set protocols ospf aggregation timer
  - set protocols ospf area area-type
  - set protocols ospf area filter-list prefix
  - set protocols ospf area no-summary
  - set protocols ospf area range
  - set protocols ospf area virtual-link
  - set protocols ospf area virtual-link authentication
  - set protocols ospf area virtual-link authentication-key
  - set protocols ospf area virtual-link dead-interval
  - set protocols ospf area virtual-link hello-interval
  - set protocols ospf area virtual-link message-digest-key md5
  - set protocols ospf area virtual-link retransmit-interval
  - set protocols ospf area virtual-link transmit-delay
  - set protocols ospf auto-cost reference-bandwidth
  - set protocols ospf compatible rfc1583
  - set protocols ospf default-information originate
  - set protocols ospf default-metric
  - set protocols ospf interface area
  - set protocols ospf interface authentication address
  - set protocols ospf interface authentication message-digest
  - set protocols ospf interface cost
  - set protocols ospf interface dead-interval
  - set protocols ospf interface hello-interval
  - set protocols ospf interface message-digest-key md5
  - set protocols ospf interface network
  - set protocols ospf interface priority
  - set protocols ospf interface retransmit-interval
  - set protocols ospf interface transmit-delay
  - set protocols ospf log-adjacency-changes
  - set protocols ospf max-metric router-lsa administrative
  - set protocols ospf max-metric router-lsa on-shutdown
  - set protocols ospf max-metric router-lsa on-startup
  - set protocols ospf multi-instance disable
  - set protocols ospf network area
  - set protocols ospf passive-interface
  - set protocols ospf redistribute
  - set protocols ospf redistribute metric-type
  - set protocols ospf redistribute route-map
  - set protocols ospf router-id
  - set protocols ospf summary-address
  - set protocols ospf timers lsa min-arrival
  - set protocols ospf timers throttle spf
  - set protocols ospf traceoption ism
  - set protocols ospf traceoption lsa
  - set protocols ospf traceoption nsm
  - set protocols ospf traceoption packet
  - set protocols ospf traceoption zebra
  - set protocols ospf graceful-restart enable
  - set protocols ospf capability opaque
  - set protocols ospf graceful-restart grace-period
  - set protocols ospf graceful-restart helper enable
  - set protocols ospf graceful-restart helper planned-only

    - set protocols ospf graceful-restart helper strict-lsa-checking
    - set protocols ospf graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf
    - run show ospf graceful-restart helper
    - set protocols ospf interface authentication-key
- OSPFv3 Command Reference
    - set protocols ospf6 area
    - set protocols ospf6 area range
    - set protocols ospf6 area stub
    - set protocols ospf6 area stub no-summary
    - set protocols ospf6 auto-cost reference-bandwidth
    - set protocols ospf6 distance
    - set protocols ospf6 distance-ospf6
    - set protocols ospf6 interface area
    - set protocols ospf6 interface cost
    - set protocols ospf6 interface dead-interval
    - set protocols ospf6 interface hello-interval
    - set protocols ospf6 interface ifmtu
    - set protocols ospf6 interface mtu-ignore
    - set protocols ospf6 interface network
    - set protocols ospf6 interface passive
    - set protocols ospf6 interface priority
    - set protocols ospf6 interface retransmit-interval
    - set protocols ospf6 interface transmit-delay
    - set protocols ospf6 log-adjacency-changes
    - set protocols ospf6 redistribute
    - set protocols ospf6 router-id
    - set protocols ospf6 stub-router administrative
    - set protocols ospf6 timers lsa min-arrival
    - set protocols ospf6 timers throttle spf
    - set protocols ospf6 traceoption
    - set protocols ospf6 traceoption border-routers
    - set protocols ospf6 traceoption lsa
    - set protocols ospf6 traceoption message
    - set protocols ospf6 traceoption neighbor
    - set protocols ospf6 traceoption route
    - set protocols ospf6 traceoption spf
    - set protocols ospf6 traceoption zebra
    - set protocols ospf6 graceful-restart enable
    - set protocols ospf6 capability opaque
    - set protocols ospf6 graceful-restart grace-period
    - set protocols ospf6 graceful-restart helper enable
    - set protocols ospf6 graceful-restart helper planned-only
    - set protocols ospf6 graceful-restart helper lsa-checking-disable
    - set protocols ospf6 graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf6
    - run show ospf6 graceful-restart helper
- Static Route Configuration Commands
    - set protocols static interface-route interface
    - set protocols static mroute
    - set protocols static route
- Route Map Commands
    - run show routing route-map
    - set routing as-path-list
    - set routing large-community-list expanded
    - set routing large-community-list standard
    - set routing prefix-list
    - set routing prefix-list description
    - set routing community-list expanded
    - set routing community-list standard
    - set routing extcommunity-list expanded
    - set routing extcommunity-list standard
    - set routing route-map set-action large-community
    - set routing route-map call
    - set routing route-map description
    - set routing route-map match as-path
    - set routing route-map match community
    - set routing route-map match community-with-exact-match
    - set routing route-map match evpn default-route
    - set routing route-map match evpn route-type
    - set routing route-map match evpn vni

- set routing route-map match extcommunity
- set routing route-map matching-policy
- set routing route-map match interface
- set routing route-map match ipv4-addr address
- set routing route-map match ipv4-addr next-hop
- set routing route-map match ipv4-addr route-source
- set routing route-map match ipv6-addr
- set routing route-map match large-community
- set routing route-map match local-preference
- set routing route-map match metric
- set routing route-map match origin
- set routing route-map match peer
- set routing route-map match source-protocol
- set routing route-map match source-vrf
- set routing route-map match tag
- set routing route-map on-match
- set routing route-map set-action aggregator
- set routing route-map set-action as-path exclude
- set routing route-map set-action as-path prepend
- set routing route-map set-action atomic-aggregate
- set routing route-map set-action comm-list-delete
- set routing route-map set-action community
- set routing route-map set-action community-additive
- set routing route-map set-action extcommunity
- set routing route-map set-action extcommunity bandwidth
- set routing route-map set-action extcommunity bandwidth-non-transitive
- set routing route-map set-action ip-next-hop
- set routing route-map set-action ipv4-vpn-next-hop
- set routing route-map set-action ipv6-next-hop
- set routing route-map set-action label-index
- set routing route-map set-action large-comm-list-delete
- set routing route-map set-action local-preference
- set routing route-map set-action metric
- set routing route-map set-action metric-type
- set routing route-map set-action origin
- set routing route-map set-action originator-id
- set routing route-map set-action src
- set routing route-map set-action tag
- set routing route-map set-action weight

- Route Leaking Commands
  - BGP Route Leaking Commands
    - set protocols bgp ipv4-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf-route-map
    - set protocols bgp vrf ipv4-unicast import vrf
    - set protocols bgp vrf ipv4-unicast import vrf-route-map
    - set protocols bgp vrf ipv6-unicast import vrf
  - Static Route Leaking Commands
    - set protocols static route nexthop-vrf next-hop
    - set protocols static vrf route nexthop-vrf next-hop

- BFD Configuration Commands
  - run show bfd
  - run show bfd counters
  - run show bfd peers
  - set protocols bfd multihop peer local-address
  - set protocols bfd multihop peer local-address detect-multiplier
  - set protocols bfd multihop peer local-address minimum-ttl
  - set protocols bfd multihop peer local-address passive-mode
  - set protocols bfd multihop peer local-address receive-interval
  - set protocols bfd multihop peer local-address shutdown
  - set protocols bfd multihop peer local-address transmit-interval
  - set protocols bfd peer detect-multiplier
  - set protocols bfd peer echo-mode
  - set protocols bfd peer echo receive-interval
  - set protocols bfd peer echo transmit-interval
  - set protocols bfd peer local-address
  - set protocols bfd peer minimum-ttl
  - set protocols bfd peer passive-mode
  - set protocols bfd peer receive-interval
  - set protocols bfd peer shutdown
  - set protocols bfd peer transmit-interval

    - set protocols bfd profile
    - set protocols bfd profile detect-multiplier
    - set protocols bfd profile echo-mode
    - set protocols bfd profile echo receive-interval
    - set protocols bfd profile echo transmit-interval
    - set protocols bfd profile minimum-ttl
    - set protocols bfd profile passive-mode
    - set protocols bfd profile receive-interval
    - set protocols bfd profile shutdown
    - set protocols bfd profile transmit-interval
    - set protocols bgp bfd
    - set protocols ospf6 interface bfd
    - set protocols ospf interface bfd
    - set protocols pim interface bfd
- Policy-Based Routing (PBR) Commands
    - set routing pbr map sequence match destination-ipv4
    - set routing pbr map sequence match source-ipv4
    - set routing pbr map sequence match destination-port
    - set routing pbr map sequence match source-port
    - set routing pbr map sequence match destination-ipv6
    - set routing pbr map sequence match source-ipv6
    - set routing pbr map sequence action nexthop
    - set routing pbr map sequence action dscp
    - set routing pbr map sequence action nexthop-group
    - set routing nexthop-group nexthop-vrf nexthop
    - set routing pbr map vlan-interface
    - run show pbr map
    - run clear pbr map
- IPv4 Source Guard (IPSG for IPv4) Commands
    - set ip-source-guard binding ip
    - set ip-source-guard enable
    - set ip-source-guard verify
    - set ip-source-guard traceoptions enable
    - run show ip-source-guard binding
- IPv6 Source Guard (IPSG for IPv6) Commands
    - set ipv6-source-guard binding ip
    - set ipv6-source-guard enable
    - set ipv6-source-guard verify
    - set ipv6-source-guard traceoptions enable
    - run show ipv6-source-guard binding
- ND Inspection Commands
    - set protocols neighbour inspection vlan disable
    - set protocols neighbour inspection validate source-mac
    - set protocols neighbour inspection trust-port
    - run show nd inspection dhcp6-snooping binding
- ND Snooping Commands
    - set protocols neighbour snooping vlan enable
    - set protocols neighbour snooping trust-port
    - set neighbour snooping max-user-number
    - set protocols neighbour snooping static-prefix vlan
    - run show neighbor snooping
    - run show neighbor snooping prefix
    - run show neighbor snooping binding
    - run clear neighbor snooping prefix
    - run clear neighbor snooping binding
- IS-IS commands
    - set protocols isis area-tag network-entity
    - set protocols isis area-tag is-type
    - set protocols isis area-tag interface
    - set protocols isis area-tag hostname-dynamic
    - set protocols isis area-tag area-password authentication-type
    - set protocols isis area-tag area-password authentication-key
    - set protocols isis area-tag area-password authenticate-snp
    - set protocols isis area-tag domain-password authentication-type
    - set protocols isis area-tag domain-password authentication-key
    - set protocols isis area-tag domain-password authenticate-snp
    - set protocols isis area-tag attached-bit receive-ignore
    - set protocols isis area-tag attached-bit send
    - set protocols isis area-tag log-adjacency-changes
    - set protocols isis area-tag metric-style
    - set protocols isis area-tag set-overload-bit
    - set protocols isis area-tag purge-originator

- set protocols isis area-tag lsp-mtu
- set protocols isis area-tag lsp-timers gen-interval
- set protocols isis area-tag lsp-timers refresh-interval
- set protocols isis area-tag lsp-timers max-lifetime
- set protocols isis area-tag spf-interval
- set protocols isis area-tag spf-delay-ietf init-delay
- set protocols isis area-tag spf-delay-ietf short-delay
- set protocols isis area-tag spf-delay-ietf long-delay
- set protocols isis area-tag spf-delay-ietf holddown
- set protocols isis area-tag spf-delay-ietf time-to-learn
- set protocols isis area-tag default-information originate
- set protocols isis area-tag default-information originate metric
- set protocols isis area-tag default-information originate route-map
- set protocols isis area-tag topology ipv6-unicast
- set protocols isis area-tag interface circuit-type
- set protocols isis area-tag interface csnp-interval
- set protocols isis area-tag interface psnp-interval
- set protocols isis area-tag interface hello-padding
- set protocols isis area-tag interface hello-interval
- set protocols isis area-tag interface hello-multiplier
- set protocols isis area-tag interface metric
- set protocols isis area-tag interface network point-to-point
- set protocols isis area-tag interface passive
- set protocols isis area-tag interface password authentication-type
- set protocols isis area-tag interface password authentication-key
- set protocols isis area-tag interface priority
- set protocols isis area-tag interface three-way-handshake
- set protocols isis area-tag interface bfd
- set protocols isis area-tag interface topology ipv6-unicast
- set protocols isis area-tag redistribute
- set protocols isis traceoption events
- set protocols isis traceoption adj-packets
- set protocols isis traceoption route-events
- set protocols isis traceoption snp-packets
- run show isis summary
- run show isis interface
- run show isis database
- run show isis hostname
- run show isis neighbor
- run show isis route
- run show isis topology

run show neighbors

The **run show neighbors** command is used to view all IPv6 neighbor entries.

Command Syntax

run show neighbors [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.

Usage Guidelines

When a VRF is specified, only the IPv6 neighbor entries of the specific VRF are displayed.

When no VRF is specified, the result shows only the IPv6 neighbor entries of the default VRF.

Example

- View all IPv6 neighbour entries.

```
admin@Xorplus# run show neighbors
Aging-time(seconds): 1200
Total count        : 1
Address   HW Address     Interface
-----------  -----------------     ---------
2001::1  22:22:22:22:22:22   vlan-2
```

run show route

The **run show route** command shows the information about the IP routing table.

Command Syntax

run show route [**vrf** *<vrf-name>* | *<ip-address>* | **ospf | bgp | static |connected | kernal | ipv4 | ipv6 | summary**]

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name. The value is a string.
<ip-address>	Optional. Specifies a destination IP address.

Usage Guidelines

When a VRF is specified, only the routing table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the routing table information of the default VRF.

Example

- View the information about the IP address 40.92.0.0/24.

```
admin@Xorplus# run show route 40.92.0.0/24
RIB entry for 40.92.0.0/24
==========================
Routing entry for 40.92.0.0/24
  Known via "ospf", distance 110, metric 10
  Last update 00:43:58 ago
    directly connected, vlan4092, weight 1

Routing entry for 40.92.0.0/24
  Known via "connected", distance 0, metric 0, best
  Last update 00:44:43 ago
  * directly connected, vlan4092


FIB entry for 40.92.0.0/24
==========================
40.92.0.0/24 dev vlan4092 proto kernel scope link src 40.92.0.1
```

- View the information about the IP routing table of OSPF protocol.

```
admin@Xorplus# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 1.1.1.1/32 [110/10] via 40.93.0.2, vlan4093, weight 1, 03:01:16
O>* 2.2.2.2/32 [110/10] via 40.94.0.2, vlan4094, weight 1, 00:00:45
O   3.3.3.3/32 [110/0] is directly connected, lo, weight 1, 05:55:08
O>* 4.4.4.4/32 [110/10] via 40.92.0.2, vlan4092, weight 1, 00:47:26
O>* 40.40.0.0/24 [110/30] via 40.92.0.2, vlan4092, weight 1, 00:00:45
  *                       via 40.94.0.2, vlan4094, weight 1, 00:00:45
O   40.92.0.0/24 [110/10] is directly connected, vlan4092, weight 1, 00:47:26
O   40.93.0.0/24 [110/10] is directly connected, vlan4093, weight 1, 03:06:18
O   40.94.0.0/24 [110/10] is directly connected, vlan4094, weight 1, 00:01:38
```

- View the information about the IP routing table of the default VRF.

```
admin@Xorplus# run show route
show ip route
=============
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 05:48:10
O>* 1.1.1.1/32 [110/10] via 40.93.0.2, vlan4093, weight 1, 02:54:17
O>* 2.2.2.2/32 [110/10] via 40.94.0.2, vlan4094, weight 1, 05:46:52
O   3.3.3.3/32 [110/0] is directly connected, lo, weight 1, 05:48:09
C>* 3.3.3.3/32 is directly connected, lo, 05:48:10
O>* 4.4.4.4/32 [110/10] via 40.92.0.2, vlan4092, weight 1, 00:40:27
C>* 10.10.51.0/24 is directly connected, eth0, 05:48:10



show ipv6 route
===============
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C * fe80::/64 is directly connected, vlan4092, 00:41:11
C * fe80::/64 is directly connected, vlan4093, 02:59:17
C * fe80::/64 is directly connected, vlan4094, 05:47:4
```

run show route forward-host

The **run show route forward-host** command shows the information about the host hardware forwarding table.

Command Syntax

run show route [**vrf** <*vrf-name*>] **forward-host brief**

run show route [**vrf** <*vrf-name*>] **forward-host ipv4** <*ipv4-address* | **all**>

run show route [**vrf** <*vrf-name*>] **forward-host ipv6** <*ipv6-address* | **all**>

Parameter

Parameter	Description
brief	Displays statistics information about host routes in the IP routing table.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.
ipv4 <*ipv4-address* | **all**>	Specifies an IPv4 address to view the host hardware forwarding table information of a specific IPv4 host, or **all** to view the host hardware forwarding table information of all IPv4 hosts.
ipv6 <*ipv6-address* | **all**>	Specifies an IPv6 address to view the host hardware forwarding table information of a specific IPv6 host, or **all** to view the host hardware forwarding table information of all IPv6 hosts.

Usage Guidelines

When a VRF is specified, only the host hardware forwarding table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the host hardware forwarding table information of the default VRF.

Example

- View the host hardware forwarding table information of all IPv4 hosts.

```
admin@Xorplus# run show route forward-host ipv4 all
Address        HWaddress        Port
---------------   -----------------       ---------
20.20.20.3     70:72:CF:9D:6F:FB   ae3
Total host count:1
```

run show route forward-route

The **run show route forward-route** command is used to view the hardware route forwarding table information.

Command Syntax

run show route [**vrf** <*vrf-name*>] **forward-route brief**

run show route [**vrf** <*vrf-name*>] **forward-route ipv4** {<*IP4Net*>| **all**}

run show route [**vrf** <*vrf-name*>] **forward-route ipv6** {<*IP6Net*>| **all**}

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.
brief	Displays statistics information about routes in the IP routing table.
ipv4 {<*IP4Net*>| **all**}	Specifies an IPv4 network segment address to view the hardware route forwarding table information of a specific IPv4 network segment, or **all** to view the hardware route forwarding table information of all IPv4 network segment.
ipv6 {<*IP6Net*>| **all**}	Specifies an IPv6 network segment address to view the hardware route forwarding table information of a specific IPv6 network segment, or **all** to view the hardware route forwarding table information of all IPv6 network segment.

Usage Guidelines

When a VRF is specified, only the hardware route forwarding table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the hardware route forwarding table information of the default VRF.

Example

- View the hardware route forwarding table information.

```
admin@Xorplus# run show route forward-route ipv4 all
Destination       NextHopMac        Port
---------------      -----------------       ---------
20.20.20.0/24    00:18:23:30:DD:53   connected
Total route count:1
```

- If IP routing function is disabled, the command result shows "**Ip routing is disable**".

```
admin@XorPlus# run show route forward-route ipv4 all
Ip routing is disable
```

run show vrf

The **run show vrf** command is used to view the binding information between the VRFs and the Layer 3 interfaces.

Command Syntax

run show vrf

Parameter

None.

Example

- View the binding information between the VRFs and the Layer 3 interfaces.

```
admin@Xorplus# run show vrf
Vrf          Description       Interfaces
----------   ---------------   -------------------------
vrf1                           vlan1,vlan2
vrf10                          vlan19,vlan20
vrf100                         vlan199,vlan200
vrf101                         vlan201,vlan202
vrf200                         r1.1,r2
```

set ip vrf

The **set ip vrf** command creates a VRF.

Command Syntax

set ip vrf <*vrf-name*> [**description** <*string*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies a VRF name. The value is a string of 1 to 15 case-sensitive characters; spaces are not supported. Note: • Keywords mgmt-vrf, default, vlan.1, ..., vlan.4094, eth0 and eth1 cannot be configured as a VRF name. • A switch supports a maximum of 128 VRFs.
description <*string*>	Optional. Add description information for the VRF. The value is a string.

Example

- Create a VRF vrf1.

```
admin@Xorplus# set ip vrf vrf1 description east
admin@Xorplus# commit
```

set ip routing enable

The **set ip routing enable** command configures whether to enable or disable IP routing function.

NOTE:

- Layer 3 packets cannot be forwarded normally if IP routing function is disabled.
- If the following commit failed message appears when you enable IP routing, the Enterprise License is not installed, and you need to purchase and install the Enterprise License before the L3 feature can be used properly.

```
admin@Xorplus# set ip routing enable true
admin@Xorplus# commit
Command failed: L3 feature is not covered by the installed license key.
Commit failed.
```

Command Syntax

set ip routing enable [**true | false**]

Parameter

Parameter	Description
enable [**true	false**]	Configures whether to enable or disable IP routing function. The value is **true** or **false**. **true**: enables the IP routing function. **false**: disables the IP routing function. The default value is **false**.

Example

- Disable the IP routing function.

```
admin@Xorplus# set ip routing enable false
admin@Xorplus# commit
```

- Enable the IP routing function.

```
admin@Xorplus# set ip routing enable true
admin@Xorplus# commit
```

set system management-vrf enable

The **set system management-vrf enable** command is used to enable or disable management VRF.

Command Syntax

set system management-vrf enable <true | false>

Parameter

Parameter	Description
enable <**true** | **false**>	Enables or disables management VRF. The value could be **true** or **false**. • **true**: enables management VRF. • **false**: disables management VRF. By default, management VRF is disabled.

Usage Guidelines

By default, PICOS starts up with only default VRF, management VRF function is disabled. To enhance the security of the management network, and prevent attacks by illegal users, users can use this command to enable management VRF. Once management VRF is enabled, a VRF with fixed name **mgmt-vrf** is created by the system, Eth0 management interface is automatically moved from the default VRF to the management VRF.

Management VRF is dedicated to transmit the management traffic. Other VRFs are used to transmit the data traffic, thus separating the management traffic from the data traffic effectively.

Example

- Enable management VRF.

```
admin@Xorplus# set system management-vrf enable true
admin@Xorplus# commit
```

BGP Commands

- run show bgp
- run show bgp neighbor
- run show bgp route
- run show bgp unicast neighbor graceful-restart
- set protocols bgp aggregate-address
- set protocols bgp always-compare-med
- set protocols bgp bestpath as-path type multipath-relax
- set protocols bgp bestpath bandwidth
- set protocols bgp bestpath compare-routerid
- set protocols bgp bestpath med missing-as-worst
- set protocols bgp cluster-id
- set protocols bgp graceful-shutdown
- set protocols bgp listen
- set protocols bgp local-as
- set protocols bgp max-med
- set protocols bgp multipath maximum-paths
- set protocols bgp neighbor activate
- set protocols bgp neighbor addpath-tx-all-paths
- set protocols bgp neighbor addpath-tx-bestpath-per-as
- set protocols bgp neighbor advertisement-interval
- set protocols bgp neighbor allowas-in
- set protocols bgp neighbor as-override
- set protocols bgp neighbor capability extended-nexthop
- set protocols bgp neighbor default-originate
- set protocols bgp neighbor description
- set protocols bgp neighbor disable-connected-check
- set protocols bgp neighbor ebgp-multihop
- set protocols bgp neighbor filter-list
- set protocols bgp neighbor next-hop-self
- set protocols bgp neighbor password
- set protocols bgp neighbor peer-group
- set protocols bgp neighbor prefix-list
- set protocols bgp neighbor remote-as
- set protocols bgp neighbor remove-private-as
- set protocols bgp neighbor route-map
- set protocols bgp neighbor route-reflector-client
- set protocols bgp neighbor send-community
- set protocols bgp neighbor shutdown
- set protocols bgp neighbor soft-reconfiguration
- set protocols bgp neighbor timers connect
- set protocols bgp neighbor timers holdtime
- set protocols bgp neighbor timers keepalive
- set protocols bgp neighbor ttl-security hops
- set protocols bgp neighbor update-source
- set protocols bgp network
- set protocols bgp network-import-check
- set protocols bgp peer-group
- set protocols bgp redistribute
- set protocols bgp route-map delay-timer
- set protocols bgp router-id
- set protocols bgp table-map
- set protocols bgp timers
- set protocols bgp update-delay
- set protocols bgp ebgp-requires-policy
- set protocols bgp neighbor timers delayopen
- set protocols bgp neighbor maximum-prefix
- set protocols bgp neighbor maximum-prefix-out
- set protocols bgp neighbor port
- set protocols bgp neighbor sender-as-path-loop-detection
- set protocols bgp fast-external-failover
- set protocols bgp confederation identifier
- set protocols bgp confederation peers
- set protocols bgp dampening

- set protocols bgp default local-preference
- set protocols bgp as-notation
- set protocols bgp neighbor local-as

run show bgp

The **run show bgp** command to displays the BGP routing table.

Command Syntax

run show bgp

Parameter

None.

Example

- View the BGP routing table.

```
admin@Xorplus# run show bgp
show bgp ipv4 unicast
=====================
BGP table version is 2, local router ID is 4.4.4.4, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0/24
                    192.168.20.1             0             100 32768 i

Displayed  1 routes and 1 total paths


show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

run show bgp neighbor

The **run show bgp neighbor** command displays information about BGP peers.

Command Syntax

run show bgp [**vrf***<vrf-name>*] **neighbor** [*<ip>* [**advertised-routes | received-routes | routes**]]

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies the VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** *<vrf-name>* [**description** *<string>*]. If not specified, displays information about BGP peers in the default VRF; If specified, displays information about BGP peers in the specified VRF.
<ip>	Optional. Specifies the IP address of a peer. If not specified, it will display information of all the BGP peers.
[**advertised-routes	received-routes	routes**]	Optional. • **advertised-routes:** Displays the routes advertised to a specified peer. • **received-routes:** Displays the routes received from a specified peer. • **route:** Displays all the routes received or advertised to a specified peer.

Example

- View the information about all the BGP peers.

```
admin@Xorplus# run show bgp neighbor
BGP neighbor on vlan20: 192.168.20.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 1.1.1.1, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  Waiting for Peer IPv6 LLA
BGP Connect Retry Timer in Seconds: 120
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.30.2, remote AS 200, local AS 200, internal link
 Administratively shut down
```

```
  BGP version 4, remote router ID 3.3.3.3, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 600 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.40.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 4.4.4.4, local router ID 2.2.2.2
  BGP state = Active
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes
```

```
  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1
```

run show bgp route

The **run show bgp route** command displays BGP route information of a specified route.

Command Syntax

run show bgp route *<ip>*

Parameter

Parameter	Description
<ip>	Specifies the IP address. It's in the form of a *ipv4-address* or *ipv6-address* or *ip-address/prefix-lenghth*.

Example

- View the BGP route information of 192.168.10.0/24.

```
admin@Xorplus# run show bgp route 192.168.10.0/24
BGP routing table entry for 192.168.10.0/24
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  192.168.50.2
  200
    192.168.10.0 from 192.168.20.1 (2.2.2.2)
      Origin IGP, metric 0, valid, external, best (First path received)
      Last update: Wed Apr  7 16:13:35 2021
```

run show bgp unicast neighbor graceful-restart

The **run show bgp unicast neighbor graceful-restart** command displays information about BGP graceful restart in the default VRF. To show information about BGP graceful restart in user-defined VRF, users can run command "**run show bgp vrf** <*vrf-name*> **neighbor** <*ip*>".

Command Syntax

run show bgp <**ipv4|ipv6**> **unicast neighbor** <*ip*> **graceful-restart**

Parameter

Parameter	Description
<**ipv4|ipv6**>	Specifies the IP type, the value could be **ipv4** or **ipv6**.
neighbor <*ip*>	Specifies the IP address of a peer. If not specified, it will display information of all the BGP peers.

Example

- View the information about BGP graceful restart.

```
admin@Xorplus# run show bgp ipv4 unicast neighbor 1.1.1.1 graceful-restart
Codes: GR - Graceful Restart, * -  Inheriting Global GR Config,
       Restart - GR Mode-Restarting, Helper - GR Mode-Helper,
       Disable - GR Mode-Disable.

Global BGP GR Mode :  Restart

BGP neighbor is 1.1.1.1
    Local GR Mode: Helper
    Remote GR Mode: NotApplicable
    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
```

set protocols bgp aggregate-address

The **set protocols bgp aggregate-address as-set** command creates an aggregate address entry in IPv4 or IPv6 format in the BGP routing table.
The **delete protocols bgp aggregate-address as-set** command removes the specified aggregate address entry.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} aggregate-address** <*ipaddress/prefixlen*> **[as-set | summary-only]**

delete protocols bgp [**vrf** <*vrf-name*>]**{ipv4-unicast|ipv6-unicast} aggregate-address** <*ipaddress/prefixlen*> **[as-set | summary-only]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
aggregate-address <*ipaddress/prefixlen*>	• *ipaddress* specifies an aggregate address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. • *ipaddress* specifies an aggregate address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
as-set	Optional. The AS_PATH attribute advertised for this route will contain an AS_SET consisting of all AS numbers contained in all paths that are being summarized.
summary-only	Optional. Creates the aggregate route but also suppresses advertisements of more-specific routes to all neighbors. This parameter can be used only for IPv6 address family type.

Example
• This example creates an aggregate address entry in the BGP routing table.

```
admin@XorPlus# set protocols bgp ipv4-unicast aggregate-address 10.0.0.0/8
admin@XorPlus# commit
```

set protocols bgp always-compare-med

The **set protocols bgp always-compare-med** command enables comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.
The **delete protocols bgp always-compare-med** command sets comparison of MED to the default setting (disabled).

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **always-compare-med**

delete protocols bgp [**vrf** <*vrf-name*>] **always-compare-med**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

- MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.
- During the best-path selection process, MED comparison is done only among paths from the same autonomous system. Use the command bgp always-compare-med to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

Example
• This example enables comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

```
admin@XorPlus# set protocols bgp always-compare-med
admin@XorPlus# commit
```

set protocols bgp bestpath as-path type multipath-relax

The **set protocols bgp bestpath as-path type multipath-relax** command configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost even if their AS-paths differ, as long as their AS-path lengths and other relevant attributes are the same. This allows routes with different AS-paths to be programmed into the forwarding table as equal cost multipath routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp bestpath as-path type multipath-relax** command restores the default behavior which configures BGP to treat two BGP routes as different costs when their AS-paths differ.

Command Syntax

set protocols bgp [***vrf***<*vrf-name*>] **bestpath as-path multipath-relax type [as-set|no-as-set]**

delete protocols bgp [***vrf***<*vrf-name*>] **bestpath as-path multipath-relax type [as-set|no-as-set]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[as-set|no-as-set]	Optional. Specifies the AS_PATH attribute advertised for this route weather contain or not contain an AS_SET. • **as-set :** The AS_PATH attribute advertised for this route will contain an AS_SET consisting of all AS numbers. • **no-as-set :** The AS_PATH attribute advertised for this route will not contain an AS_SET.

Example

• This example configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost without considering the AS-paths value.

```
admin@XorPlus# set protocols bgp bestpath as-path multipath-relax
admin@XorPlus# commit
```

set protocols bgp bestpath bandwidth

The **set protocols bgp bestpath bandwidth** command can be used to control link bandwidth processing on the receiver.
The **delete protocols bgp bestpath bandwidth** command disables the link bandwidth controlling processing on the receiver.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **bestpath bandwidth <ignore|skip-missing|default-weight-for-missing>**

delete protocols bgp [***vrf*** <*vrf-name*>] **bestpath bandwidth <ignore|skip-missing|default-weight-for-missing>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
bandwidth <ignore|skip-missing|default-weight-for-missing>	Specifies link bandwidth controlling processing on the receiver. The different options imply behavior as follows: • ignore: Ignore link bandwidth completely for route installation (i.e., do regular ECMP, not weighted) • skip-missing: Skip paths without link bandwidth and do UCMP among the others (if at least some paths have link-bandwidth) • default-weight-for-missing: Assign a low default weight (value 1) to paths not having link bandwidth

Usage Guidelines

This configuration is per BGP instance similar to other BGP route-selection controls; it operates on both IPv4-unicast and IPv6-unicast routes in that instance. In an EVPN network, this configuration (if required) should be implemented in the tenant VRF and is again applicable for IPv4-unicast and IPv6-unicast, including the ones sourced from EVPN type-5 routes.

Example
• This example is a FRR configuration on a receiver to skip paths without link bandwidth.

```
admin@XorPlus# set protocols bgp bestpath bandwidth skip-missing
admin@XorPlus# commit
```

set protocols bgp bestpath compare-routerid

The **set protocols bgp bestpath compare-routerid** command configures a BGP routing process to compare identical routes received from different external peers during the best path selection process and selects the route with the lowest router ID as the best path. Defaults to disabled.
Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.
The **delete protocols bgp bestpath compare-routerid** command returns the BGP routing process to the default operation. By default, BGP selects the route that was received first when two routes with identical attributes are received.

Command Syntax

set protocols bgp [***vrf***<*vrf-name*>] **bestpath compare-routerid**

delete protocols bgp [***vrf***<*vrf-name*>] **bestpath compare-routerid**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example configures a BGP routing process to compare identical routes received from different external peers during the best path selection process and selects the route with the lowest router ID as the best path.

```
admin@XorPlus# set protocols bgp bestpath compare-routerid
admin@XorPlus# commit
```

set protocols bgp bestpath med missing-as-worst

The **set protocols bgp bestpath med missing-as-worst** command configures a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute. The path without a MED value is the least desirable path. Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.

The **delete protocols bgp bestpath med missing-as-worst** command restores default behavior. The default behavior assigns a value of 0 to the missing MED.

Command Syntax

set protocols bgp [***vrf*** <*vrf-name*>] **bestpath med missing-as-worst**

delete protocols bgp [***vrf*** <*vrf-name*>] **bestpath med missing-as-worst**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

• This example configures a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute.

```
admin@XorPlus# set protocols bgp bestpath med missing-as-worst
admin@XorPlus# commit
```

set protocols bgp cluster-id

The **set protocols bgp cluster-id** command specifies the cluster ID when the BGP router is used as a route-reflector. The cluster ID default is the router ID. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp cluster-id**command sets the cluster ID to the default value, which is the router ID.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **cluster-id** <*IPV4-ADDR*>

delete protocol bgp [**vrf** <*vrf-name*>] **cluster-id** <*IPV4-ADDR*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<*IPV4-ADDR*>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.

Example

• This example specifies the cluster ID when the BGP router is used as a route-reflector.

```
admin@XorPlus# set protocols bgp cluster-id 2.2.2.2
admin@XorPlus# commit
```

set protocols bgp graceful-shutdown

The **set protocols bgp graceful-shutdown** command enable graceful shutdown. To reduce packet loss during planned maintenance of a router or link, you can configure graceful BGP shutdown, which forces traffic to route around the BGP node.
The **delete protocols bgp graceful-shutdown** command disables graceful BGP shutdown.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **graceful-shutdown**

delete protocols bgp [**vrf** <*vrf-name*>] **graceful-shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example enables graceful shutdown.

```
admin@XorPlus# set protocols bgp graceful-shutdown
admin@XorPlus# commit
```

set protocols bgp listen

The **set protocols bgp listen** command configures BGP dynamic neighbors listen parameters.
The **delete protocols bgp listen** command removes the configuration of BGP dynamic neighbors listen parameters.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **listen** [**limit** <*limit-number*>| **range** <*listen-range*> [**peer-group** <*peer-group*>]]

delete protocols bgp [**vrf** <*vrf-name*>] **listen [limit** <*limit-number*>| **range**<*listen-range*> [**peer-group** <*peer-group*>]**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
limit <*limit-number*>	Optional. Specifies the number of dynamic peers. The value is an integer that ranges from 1 to 5000. The default value is 100.
range<*listen-range*>	Optional. Specifies the BGP dynamic neighbors listen range. The value is in the format of <*ipaddress/prefixlen*>. • *ipaddress* specifies an aggregate address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. • *ipaddress* specifies an aggregate address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. When specifying the BGP dynamic neighbors listen range, you can also set the peer group.

Example
• This example limits the number of dynamic peers to 5.

```
admin@XorPlus# set protocols bgp listen limit 5
admin@XorPlus# commit
```

set protocols bgp local-as

Users can set the Autonomous System (AS) number for this domain.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>
delete protocols bgp [vrf <*vrf-name*> **local-as** <*AS-NUMBER*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
local-as <*AS-NUMBER*>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example sets AS number as 5:

```
admin@XorPlus# set protocols bgp local-as 5
admin@XorPlus# commit
```

set protocols bgp max-med

The **set protocols bgp max-med** command sets that advertise routes with max-med attribute.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **max-med [administrative med** <*AS-NUMBER*>| **on-startup [duration** <*period*> **| med** <*AS-NUMBER*>**]]**
delete protocols bgp [vrf <*vrf-name*> **max-med [administrative med** <*AS-NUMBER*>**| on-startup [duration** <*period*> **| med** <*AS-NUMBER*>**]]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
administrative med <*AS-NUMBER*>	Optional. Specifies a 4-byte AS number in asplain format (z), where z is a number from 0 to 4294967295. Note that this is administratively applied, for an indefinite period.
duration <*period*>	Optional. Specifies the time period for max-med, which will be effective on a startup. The value is an integer, in seconds, that rangs from 5 to 86400 seconds.
med <*AS-NUMBER*>	Optional. Specifies the Max MED value to be used on a startup. The value is an integer that rangs from 0 to 4294967295.

Example
• This example sets advertise routes with max-med attribute, where Max MED value is 120.

```
admin@XorPlus# set protocols bgp max-med administrative med 120
admin@XorPlus# commit
```

set protocols bgp multipath maximum-paths

The **set protocols bgp multipath maximum-paths** command configures the maximum number of paths that BGP adds to the route table for equal-cost multipath (ECMP) load balancing for routes learned from either internal or external BGP. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp multipath maximum-paths** command restores the default setting.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **{ipv4-unicast | ipv6-unicast} multipath** {**ibgp | ebgp} maximum-paths** <*MAXPATHS*>

delete protocol bgp [**vrf** <*vrf-name*>] **{ipv4-unicast | ipv6-unicast} multipath** {**ibgp | ebgp}** [**maximum-paths]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast | ipv6-unicast}	Specifies the IPv4 unicast or IPv6 unicast.
{**ibgp | ebgp}**	Specifies the internal or external BGP.
<*MAXPATHS*>	Specifies the maximum number of paths. You can set a value between 1 and 32. 1 disables the BGP multipath option.

Example

• This example changes the maximum number of paths to 12.

```
admin@XorPlus# set protocols bgp ipv4-unicast multipath ibgp maximum-paths 12
admin@XorPlus# commit
```

set protocols bgp neighbor activate

The **set protocols bgp neighbor activate** command enables the address-family capability and exchange of information specific to an address family with a BGP neighbor.
The **delete protocols bgp neighbor activate** command removes the address-family capability and disables the exchange of routes for the specified address-family with the BGP neighbor.

> For IPv6 BGP configuration, the following command must be configured to enable the IPv6 address family capability and exchange of information specific to an IPv6 address family with a BGP neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **activate <true | false>**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **activate**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
<true | false>	Enables or disables the address-family capability. The value could be **true** or **false**. • **true**: enables the address-family capability. • **false**: disables the address-family capability.

Example
• This example enables the address-family capability and exchange of information specific to an address family with a BGP neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast activate true
admin@XorPlus# commit
```

set protocols bgp neighbor addpath-tx-all-paths

The **set protocols bgp neighbor addpath-tx-all-paths** command advertises all known paths to a neighbor.
The **delete protocols bgp neighbor addpath-tx-all-paths** command disables the additional path feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-all-paths**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-all-paths**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example

• This example advertises all known paths to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast addpath-tx-all-paths
admin@XorPlus# commit
```

set protocols bgp neighbor addpath-tx-bestpath-per-as

The **set protocols bgp neighbor addpath-tx-bestpath-per-as** command advertises only the best path learned from each AS to a neighbor.
The **delete protocols bgp neighbor addpath-tx-bestpath-per-as** command disables the additional path feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-bestpath-per-as**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-bestpath-per-as**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example advertises only the best path learned from each AS to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast addpath-tx-bestpath-per-as
admin@XorPlus# commit
```

set protocols bgp neighbor advertisement-interval

The **set protocols bgp neighbor advertisement-interval** command sets the advertisement interval, which defines the length of time between transmission of BGP routing updates.

The **delete protocols bgp neighbor advertisement-interval** command restores the default value. Default values are 30 seconds for external BGP peer and 5 seconds for internal BGP peer.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} advertisement-interval** <*advert-interval*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} advertisement-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
advertisement-interval <*advert-interval*>	Specifies the advertisement interval in seconds. Range: 0 to 600. Default: 30 for external BGP peer and 5 for internal BGP peer.

Example

• This example sets the advertisement interval to 20 seconds.

```
admin@XorPlus# set protocols bgp neighbor 1.1.1.1 advertisement-interval 20
admin@XorPlus# commit
```

set protocols bgp neighbor allowas-in

The **set protocols bgp neighbor allowas-in** command specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP speaker and still be accepted. When this configuration is applied to a peer-group, all the neighbors that are part of the peer-group inherit this setting.
The **delete protocols bgp neighbor allowas-in** command restores the default setting, which is to reject as a loop any route where the path contains the speaker AS number.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **allowas-in {**<*LIMIT*>**|origin}**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **allowas-in {**<*LIMIT*>**|origin}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
allowas-in {<*LIMIT*>**|origin}**	<*LIMIT*>*:* Specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP. Range: 1 to 10. **origin:** The parameter origin configures BGP to only accept routes originated with the same AS number as the system. This command is only allowed for eBGP peers.

Example
• This example specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP speaker and still be accepted.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast allowas-in 5
admin@XorPlus# commit
```

set protocols bgp neighbor as-override

The **set protocols bgp neighbor as-override** command overrides AS number of the originating router with the local AS number.
The **delete protocols bgp neighbor as-override** command restores the default setting.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **as-override**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **as-override**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

Usually this configuration is used in PEs (Provider Edge) to replace the incoming customer AS number so the connected CE (Customer Edge) can use the same AS number as the other customer sites. This allows customers of the provider network to use the same AS number across their sites.
This command is only allowed for eBGP peers.

Example
• This example overrides AS number of the originating router with the local AS number.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast as-override
admin@XorPlus# commit
```

set protocols bgp neighbor capability extended-nexthop

The **set protocols bgp neighbor capability extended-nexthop** command enables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings, adding the extended-nexthop capability to the global IPv6 neighbor statements on each end of the BGP sessions.
The **delete protocols bgp neighbor capability extended-nexthop** command disables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} capability extended-nexthop**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} capability extended-nexthop**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

Allow BGP to negotiate the extended-nexthop capability with it's peer. If you are peering over a IPv6 link-local address then this capability is turned on automatically. If you are peering over a IPv6 Global Address then turning on this command will allow BGP to install IPv4 routes with IPv6 nexthops if you do not have IPv4 configured on interfaces.

Example

• This example enables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 capability extended-nexthop
admin@XorPlus# commit
```

set protocols bgp neighbor default-originate

The **set protocols bgp neighbor default-originate** command enables the local router to send the default route 0.0.0.0 to a neighbor. The neighbor can then use this route to reach the router when all other routes are unavailable.
The **delete protocols bgp neighbor default-originate** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **default-originate [route-map** <*MAP-NAME*>**]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **default-originate [route-map** <*MAP-NAME*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
route-map <*MAP-NAME*>	Optional. Sets the route map to modify the default route attributes.

Example

• This example enables the local router to send the default route 0.0.0.0 to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast default-originate
admin@XorPlus# commit
```

set protocols bgp neighbor description

The **set protocols bgp neighbor description** command configures a description for a peer or peer group.

The **delete protocols bgp neighbor description** command deletes the description of a peer or peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} description <***description-text***>**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} *description* <***description-text***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
description <*description-text***>**	Specifies a description. The value is a string.

Example
• Configure a description for a peer.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 description Leaf1
admin@XorPlus# commit
```

set protocols bgp neighbor disable-connected-check

The **set protocols bgp neighbor disable-connected-check** command allows peerings between directly connected eBGP peers using loopback addresses.
The **delete protocols bgp neighbor disable-connected-check** command doesn't allow peerings between directly connected eBGP peers using loopback addresses.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} disable-connected-check**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} disable-connected-check**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example allows peerings between directly connected eBGP peers using loopback addresses.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 disable-connected-check
admin@XorPlus# commit
```

set protocols bgp neighbor ebgp-multihop

The **set protocols bgp neighbor ebgp-multihop** command enables BGP to establish a session with external peers residing on networks that are not directly connected. By default, BGP can only establish sessions with external BGP peers that are directly connected. The neighbor connection must be reset using clear bgp to allow this configuration to take effect.

The **delete protocols bgp neighbor ebgp-multihop** command disables the peer ebgp-multihop feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*>**} ebgp-multihop** [**maximum-hop** <*HOP-COUNT*>]

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*>**} ebgp-multihop** [**maximum-hop** <*HOP-COUNT*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
maximum-hop <*HOP-COUNT*>	Optional. Specifies the maximum number of hops to reach the peer. The value is an integer that ranges from 1 to 255.

Example
• This example enables BGP to establish connection with external peers residing on networks that are not directly connected:

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ebgp-multihop maximum-hop 5

admin@XorPlus# commit
```

set protocols bgp neighbor filter-list

The **set protocols bgp neighbor filter-list** command configures an AS Path list to advertise or receive routes from peers.

The **delete protocols bgp neighbor filter-list** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} filter-list** <*as-path-list*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} filter-list** <*as-path-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
filter-list <*as-path-list*>	Specifies the AS Path list, which is configured by the command **set routing as-path-list**.
{in|out}	Sets the filter policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example
• This example configures an AS Path list to receive routes from peers.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in filter-list List1
admin@XorPlus# commit
```

set protocols bgp neighbor next-hop-self

The **set protocols bgp neighbor next-hop-self** command configures the router as the next hop for a BGP-speaking neighbor or peer group, and enables BGP to send itself as the next hop for advertised routes.
The **delete protocols bgp neighbor next-hop-self** command resets the peer nexthop-self status to default. The next hop will be generated based on the IP.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **next-hop-self [force]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **next-hop-self [force]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example configures the router as the next hop for a BGP-speaking neighbor or peer group, and enables BGP to send itself as the next hop for advertised routes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast next-hop-self
admin@XorPlus# commit
```

set protocols bgp neighbor password

The **set protocols bgp neighbor password** command enables message digest5 (MD5) authentication on a TCP connection between two BGP neighbors. When the password is applied to a peer-group, all the neighbors that are part of peer-group inherit the configured
setting. The neighbor connection must be reset using clear ip bgp to allow this configuration to take effect.

The **delete protocols bgp neighbor password** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} password** <*text-password*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} password**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
password <*text-password*>	Specifies the txt password.

Example
• This example enables message digest5 (MD5) authentication on a TCP connection between two BGP neighbors.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 password picos12345
admin@XorPlus# commit
```

set protocols bgp neighbor peer-group

The **set protocols bgp neighbor peer-group** command adds a peer to a peer group.
The **delete protocols bgp neighbor peer-group** command removes a peer to a peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*> | **interface** <*interface*>**} peer-group** <*peergroup*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*> | **interface** <*interface*>**} peer-group** <*peergroup*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
peer-group <*peergroup*>	Specifies a peer group name. The value is a string.

Usage Guidelines

Instead of specifying properties of each individual peer, you can define one or more peer groups and associate all the attributes common to that peer session to a peer group. A peer needs to be attached to a peer group only once, when it then inherits all address families activated for that peer group.

Note:

If the peer you want to add to a group already exists in the BGP configuration, delete it first, than add it to the peer group.

Example

• This example adds two peers to a peer group **leaf1**.

```
admin@XorPlus# set protocols bgp neighbor 10.10.0.1 peer-group leaf1
admin@XorPlus# set protocols bgp neighbor 10.10.0.12 peer-group leaf1
admin@XorPlus# commit
```

set protocols bgp neighbor prefix-list

The **set protocols bgp neighbor prefix-list** command configures an IPv4 or IPv6 prefix list to advertise or receive routes from peers.

The **delete protocols bgp neighbor prefix-list** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} prefix-list** <*prefix-list*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} prefix-list** <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4 or IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
prefix-list <*prefix-list*>	Specifies the IPv4 or IPv6 prefix list.
{in|out}	Sets the filter policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example

• This example configures an IPv4 prefix list to receive routes from peers.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in prefix-list List1
admin@XorPlus# commit
```

set protocols bgp neighbor remote-as

The **set protocols bgp neighbor remote-as** command creates a peer, initiates the connection to the peer, and adds an entry to the BGP neighbor table. Specifies a neighbor with an autonomous system (AS) number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command, exchange only unicast address prefixes.
The **delete protocols bgp neighbor remote-as** command disables the peer session and deletes the peer information.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} remote-as {**<*as-number*>**|external|internal}**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} remote-as {**<*as-number*>**|external|internal}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
remote-as {<*as-number*>**|external|internal}**	<*as-number*>: Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535. **external**: Create a peer as you would when you specify an ASN, except that if the peers ASN is the same as mine as specified under this command the connection will be denied. **internal**: Create a peer as you would when you specify an ASN, except that if the peers ASN is different than mine as specified under tis command the connection will be denied.

Example
• This example specifies a neighbor with an autonomous system (AS) number.

```
admin@XorPlus# set protocols bgp neighbor 10.10.0.1 remote-as 100
admin@XorPlus# commit
```

set protocols bgp neighbor remove-private-as

The **set protocols bgp neighbor remove-private-as** command removes private ASNs from routes sent to the neighbor.

The **delete protocols bgp neighbor remove-private-as** command allows the private-AS number to be carried in BGP update message.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **remove-private-as [all] [replace-as]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} {ipv4 unicast|ipv4 labeled-unicast|ipv6 unicast|ipv6 labeled-unicast} remove-private-as [all] [replace-as]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
[all]	Optional. Apply to all AS numbers.
[replace-as]	Optional. Replaces the private ASNs with your public ASN.

Usage Guidelines

If you use private ASNs in the data center, any routes you send out to the internet contain your private ASNs. You can remove all the private ASNs from routes to a specific neighbor.

Example

• This example removes private ASNs from routes sent to the neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast remove-private-as
admin@XorPlus# commit
```

set protocols bgp neighbor route-map

The **set protocols bgp neighbor route-map** command applies a route map to incoming or outgoing routes. It configures the route map for modifying the default attributes of the route. The **delete protocols bgp neighbor route-map** command removes a route map.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} route-map** <*route-map*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} route-map** <*route-map*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
route-map <*route-map*>	Specifies the name of the route map.
{in|out}	Sets the route map policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example

• This example applies a route map to the incoming routes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in route-map map1
admin@XorPlus# commit
```

set protocols bgp neighbor route-reflector-client

The **set protocols bgp neighbor route-reflector-client** command configures the router as a BGP route reflector and the specified peer as its client.
The **delete protocols bgp neighbor route-reflector-client** command disables this function.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **route-reflector-client**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **route-reflector-client**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example configures the router as a BGP route reflector and the specified peer as its client.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast route-reflector-client
admin@XorPlus# commit
```

set protocols bgp neighbor send-community

The **set protocols bgp neighbor send-community** command enables community and/or extended community exchange with the specified neighbor. When this command is configured for the peer-group, then all the neighbors that are part of peer-group will send the community values to the peers.
The **delete protocols bgp neighbor send-community** command will not allow the neighbor to send community values to the specific neighbors that are part of peer-group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **send-community type [both|extended|standard|large|all]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **send-community type [both|extended|standard|large|all]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
[both|extended|standard|large|all]	Optional. The parameters **standard**, **large** and **extended** send only the respective community numbers. **all**: both standard and extended communities will be sent to the neighbor.

Example
• This example allows community values to be sent to a specific neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast send-community type both
admin@XorPlus# commit
```

set protocols bgp neighbor shutdown

The **set protocols bgp neighbor shutdown** command disables the peer session, terminates any active session for the specified neighbor or peer group, and removes all associated routing information. This action can cause the sudden termination of many peering sessions.

The **delete protocols bgp neighbor shutdown** command enables the peer session for the specified neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} shutdown**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines
Sessions are gracefully shut down when graceful-shutdown is enabled. Use the set protocols bgp graceful-shutdown command to enable graceful-shutdown. If graceful-shutdown is configured without delay or localpreference, the default values are used.

Example
• This example disables the peer session for the specified neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 shutdown
admin@XorPlus# commit
```

set protocols bgp neighbor soft-reconfiguration

The **set protocols bgp neighbor soft-reconfiguration** command enables you to generate inbound updates from a neighbor and change and activate BGP policies without clearing the BGP session. Changes in BGP policies require the BGP session to be cleared which can have a large negative impact on network operations.
The **delete protocols bgp neighbor soft-reconfiguration** command disables this setting.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **soft-reconfiguration inbound**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **soft-reconfiguration inbound**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

- To perform inbound soft reconfiguration, the BGP speaker must store all received route updates, regardless of the current inbound policy.
- When inbound soft reconfiguration is enabled, the stored updates are processed by the new policy configuration to create new inbound updates.

Example

• This example enables to generate inbound updates from a neighbor and change and activate BGP policies without clearing the BGP session.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast soft-reconfiguration inbound
admin@XorPlus# commit
```

set protocols bgp neighbor timers connect

By default, the BGP process attempts to connect to a peer after a failure (or on startup) every 10 seconds. You can change this value to suit your needs.

The **set protocols bgp neighbor timers connect** command sets the reconnect value.
The **delete protocols bgp neighbor timers connect** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers connect** <*timers*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers connect**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
timers connect <*timers*>	Specifies the reconnect timer value for the neighbor. Default: 10 seconds. Range: 1-65535.

Example
• This example sets the reconnect value to 30 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers connect 30
admin@XorPlus# commit
```

set protocols bgp neighbor timers holdtime

The **set protocols bgp neighbor timers connect holdtime** command sets the hold time for a BGP peer.
The **delete protocols bgp neighbor timers connect holdtime** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers holdtime** <*hold time*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers holdtime**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
<*hold time*>	Specifies the hold time. Default: 180 seconds. Range: 0-65535.

Usage Guidelines

By default, BGP exchanges periodic keepalive messages to measure and ensure that a peer is still alive and functioning. If a keepalive or update message is not received from the peer within the hold time, the peer is declared down and all routes received by this peer are withdrawn from the local BGP table. By default, the keepalive interval is set to 60 seconds and the hold time is set to 180 seconds. To decrease CPU load, especially in the presence of a lot of neighbors, you can increase the values of these timers or disable the exchange of keepalives entirely. When manually configuring new values, the keepalive interval can be less than or equal to one third of the hold time, but cannot be less than 1 second. Setting the keepalive and hold time values to 0 disables the exchange of keepalives.

Example
• This example set the hold time to 200 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers holdtime 200
admin@XorPlus# commit
```

set protocols bgp neighbor timers keepalive

The **set protocols bgp neighbor timers connect keepalive** command sets the keepalive interval for a BGP peer.
The **delete protocols bgp neighbor timers connect keepalive** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers keepalive** <*keepalive interval*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers keepalive**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
keepalive <*keepalive interval*>	Specifies the keepalive interval value for the neighbor. Default: 60 seconds. Range: 0-65535.

Usage Guidelines

By default, BGP exchanges periodic keepalive messages to measure and ensure that a peer is still alive and functioning. If a keepalive or update message is not received from the peer within the hold time, the peer is declared down and all routes received by this peer are withdrawn from the local BGP table. By default, the keepalive interval is set to 60 seconds and the hold time is set to 180 seconds. To decrease CPU load, especially in the presence of a lot of neighbors, you can increase the values of these timers or disable the exchange of keepalives entirely. When manually configuring new values, the keepalive interval can be less than or equal to one third of the hold time, but cannot be less than 1 second. Setting the keepalive and hold time values to 0 disables the exchange of keepalives.

Example
• This example set the keepalive interval to 80 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers keepalive 80
admin@XorPlus# commit
```

set protocols bgp neighbor ttl-security hops

The **set protocols bgp neighbor ttl-security hops** command enables BGP to establish connection with external peers residing on networks that are not directly connected. By enabling this feature, the received TTL from a BGP peer is compared with the difference "255 - hop-count". BGP messages coming with a TTL less than this value are not accepted. BGP peering will not be established if the TTL in the session establishment is received with a lower value. Also, by enabling this feature the router will send BGP packets with TTL value of 255 to the neighbor. For a neighbor, either TTL security or ebgp-multihop can be configured, not both together. If there are multiple paths to reach the node, then the hop count should be configured considering the longest route.

The **delete protocols bgp neighbor ttl-security hops** command disables the peer ttl-security-hop feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} ttl-security hops** <*HOP-COUNT*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} ttl-security hops** <*HOP-COUNT*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
ttl-security hops <*HOP-COUNT*>	Specifies the hop count to reach the neighbor for the eBGP session. Range: 1-254.

Example
• This example enables the peer ttl-security-hop feature.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ttl-security hops 10
admin@XorPlus# commit
```

set protocols bgp neighbor update-source

The **set protocols bgp neighbor update-source** command specifies the source address to reach the neighbor. An iBGP connection can occur as long as there is a TCP/IP path between the routers. If multiple paths exist between the iBGP routers, using a loopback interface as the neighbor address can add stability to the network. With this command, stability can be achieved by providing the loopback interface address as the source address of the TCP/IP session.

The **delete protocols bgp neighbor update-source** command negates the route updates of the neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} update-source** {<*IPv4*>|<*IPv6*> |<*interface-source*>}

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} update-source**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
update-source {<*IPv4*>|<*IPv6*> |<*interface-source*>}	Specifies the source address or source interface. • <*IPV4*>: Specifies an interface by IPv4 address. • <*IPV6*>: Specifies an interface by IPv6 address. • <*interface-source*>: Specifies a source interface name.

Example

• This example specifies the source address to reach the neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 update-source 10.10.192.1
admin@XorPlus# commit
```

set protocols bgp network

The **set protocols bgp network** command specifies the IPv4/IPv6 networks to be advertised by the Border Gateway Protocol (BGP) routing processes.
The **delete protocols bgp network** command removes an entry from the routing table.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network <***ip-address/prefixlen*> **[label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]**

delete protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network** <*ip-address/prefixlen*> **[label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
<*ip-address/prefixlen*>	Specifies the IPv4/IPv6 network with mask. For example: 1.1.1.0/24
label-index <*label-index*>	Optional parameter. Specifies a route label.
route-map <*ROUTE-MAP-NAME*>	Optional parameter. Specifies a route map to apply to the prefixes advertised by this specific network statement.

Usage Guidelines
• This command is used to advertise prefixes currently installed in the routing table into the BGP table.
• Use the route-map keyword to apply the specified route map to network advertisements. The mask length as configured in the network statement must match the mask length of prefixes in the routing table.

Example
• This example specifies the networks to be advertised by the Border Gateway Protocol (BGP) routing processes.

```
admin@XorPlus# set protocols bgp ipv4-unicast network 11.11.11.0/24
admin@XorPlus# commit
```

set protocols bgp network-import-check

The **set protocols bgp network-import-check** command modifies the behavior of the network statement. If you have this configured the underlying network must exist in the rib.
The **delete protocols bgp network-import-check** command sets that BGP will not check for the networks existence in the rib.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **network-import-check**

delete protocols bgp [**vrf** <*vrf-name*>] **network-import-check**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example modifies the behavior of the network statement.

```
admin@XorPlus# set protocols bgp network-import-check
admin@XorPlus# commit
```

set protocols bgp peer-group

The **set protocols bgp peer-group** command creates a peer group.
The **delete protocols bgp peer-group** command deletes a peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **peer-group** <*peer-group*>

delete protocols bgp [**vrf** <*vrf-name*>] **peer-group** <*peer-group*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer-group <*peer-group*>	Specifies a name of peer group.

Usage Guidelines

Instead of specifying properties of each individual peer, you can define one or more peer groups and associate all the attributes common to that peer session to a peer group. A peer needs to be attached to a peer group only once, when it then inherits all address families activated for that peer group.

Note:

If the peer you want to add to a group already exists in the BGP configuration, delete it first, than add it to the peer group.

Example

• This example creates a peer group.

```
admin@XorPlus# set protocols bgp peer-group leaf1
admin@XorPlus# commit
```

set protocols bgp redistribute

The **set protocols bgp redistribute** command specifies IPv4/IPv6 routes to import into BGP. This command causes routes from the specified protocol to be considered for redistribution into BGP.
The **delete protocols bgp redistribute** command deletes the routes imported into BGP.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|isis|rip|static|table <***table-number***>**} [**metric** <*metric-number*>|**route-map** <*route-map*>]

delete protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|isis|rip|static|table** <*table-number*>} [**metric** <*metric-number*>|**route-map** <*route-map*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
redistribute {**connected|kernel|ospf|isis|rip|static|table|table <***table-number***>**}	Redistributes routes to import into BGP. • **connected**: Redistribute connected route to BGP process. • **kernel**: Redistribute kernel route to BGP process. • **ospf**: Redistribute OSPFv2 route to BGP process. • **isis**: Redistribute IS-IS route to BGP process. • **rip**: Redistribute RIP route to BGP process. • **static**: Redistribute static route to BGP process. • **table <***table-number***>**: Redistribute specific route table to BGP process. The value is an integer that ranges from 1 to 65535.
metric <*metric-number*>	Optional. Specifies route metric of the imported routes into BGP. The value is an integer that ranges from 0 to 4294967295.
route-map <*route-map*>	Optional. Specifies the name of the route map.

Example
• This example redistributes OSPF route to BGP process, and the route metric is set to 20.

```
admin@XorPlus# set protocols bgp ipv4-unicast redistribute ospf metric 20
admin@XorPlus# commit
```

set protocols bgp route-map delay-timer

The **set protocols bgp route-map delay-timer** command sets the delay before any route-maps are processed.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **route-map delay-timer** <*delay-timer*>
delete protocols bgp [**vrf** <*vrf-name*> **route-map delay-timer** <*delay-timer*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
delay-timer <*delay-timer*>	Specifies a delay timer. The value is an integer, in second, that ranges from 0 to 600. The default time for this is 5 seconds.

Example
• This example sets the delay before any route-maps are processed.

```
admin@XorPlus# set protocols bgp route-map delay-timer 10
admin@XorPlus# commit
```

set protocols bgp router-id

The **set protocols bgp router-id** command configures a Router ID for the switch.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **router-id** <*router-id*>
delete protocols bgp [**vrf** <*vrf-name*> **router-id** <*router-id*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
router-id <*router-id*>	Specifies a Router ID. It is in dotted decimal notation.

Example
• Configure a Router ID for the switch.

```
admin@XorPlus# set protocols bgp router-id 10.1.1.1
admin@XorPlus# commit
```

set protocols bgp table-map

The **set protocols bgp table-map** command is used to apply a route-map on route updates from BGP to Zebra. All the applicable match operations are allowed, such as match on prefix, next-hop, communities, etc. Set operations for this attach-point are limited to metric and next-hop only. Any operation of this feature does not affect BGPs internal RIB. Supported for ipv4 and ipv6 address families. It works on multi-paths as well, however, metric setting is based on the best-path only.
The **delete protocols bgp table-map** command disables this feature.

Command Syntax

set protocol bgp [vrf <*text*>**] {ipv4-unicast|ipv6-unicast} table-map** <*route-map-name*>

delete protocol bgp [vrf <*text*>**] {ipv4-unicast|ipv6-unicast} table-map** <*route-map-name*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Specifies the IP address family type.
table-map <*route-map-name*>	Specifies the name of the route map.

Example
• This example applies a route-map on route updates from BGP to Zebra.

```
admin@XorPlus# set protocols bgp ipv4-unicast table-map map1
admin@XorPlus# commit
```

set protocols bgp timers

The **set protocols bgp timers** command sets the timers for all the BGP neighbor.

The **delete protocols bgp timers** command clears the BGP timers.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **timers {holdtime** <*HOLDTIME*>**|keepalive** <*KEEPALIVE*>**}**

delete protocols bgp [**vrf** <*vrf-name*> **timers {holdtime** <*HOLDTIME*>|**keepalive**<*KEEPALIVE*>}

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
keepalive<*KEEPALIVE*>	Specifies the Keep-Alive timer value for the neighbor. Default: 60 seconds. Range: 0-65535.
holdtime <*HOLDTIME*>	Specifies the Hold-timer value. Default: 180 seconds. Range: 0-65535.

Example

• This example sets the keepalive timer for all the BGP neighbor.

```
admin@XorPlus# set protocols bgp timers keepalive 360
admin@XorPlus# commit
```

set protocols bgp update-delay

The **set protocols bgp update-delay** command enable read-only mode by setting the maximum delay timer.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **update-delay {delay** <*maximum delay-timer*>| **establish-wait** <*establish-wait-timer*>}
delete protocols bgp [**vrf** <*vrf-name*> **update-delay delay [delay** <*maximum delay-timer*>| **establish-wait** <*establish-wait-timer*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
delay <*maximum delay-timer*>	Specifies a maximum delay timer. The value is an integer, in second, that ranges from 0 to 3600. The default time for this is 0 seconds, which disables read-only mode.
establish-wait <*establish-wait-timer*>	Optional. Specifies a establish wait timer. The value is an integer, in second, that ranges from 0 to 3600. When specified, it should be less than the maximum delay timer.

Usage Guidelines

To enable read-only mode, you set the maximum delay timer and, optionally, the establish-wait timer. Read-only mode begins as soon as the first peer reaches its established state and the maximum delay timer starts, and continues until either of the following two conditions are met:

- All the configured peers (except the shutdown peers) have sent an explicit EOR (End-Of-RIB) or an implicit EOR. The first keep-alive after BGP reaches the established state is considered an implicit EOR. If you specify the *establish-wait* option, BGP only considers peers that have reached the established state from the moment the maximum delay timer starts until the establish-wait period ends. The minimum set of established peers for which EOR is expected are the peers that are established during the establish-wait window, not necessarily all the configured neighbors.
- The timer reaches the configured maximum delay.

Example
• The following example commands enable read-only mode by setting the maximum delay timer to 300 seconds.

```
admin@XorPlus# set protocols bgp update-delay delay 300
admin@XorPlus# commit
```

set protocols bgp ebgp-requires-policy

The **set protocols bgp ebgp-requires-policy** command determines whether or not EBGP will exchange routes with peers by using a policy.

The **delete protocols bgp ebgp-requires-policy** command restores the default configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **ebgp-requires-policy** <**true | false**>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true	false**>	Enable or disable ebgp-requires-policy. The value could be **true** or **false**. • **true**: Enable ebgp-requires-policy. • **false**: Disable ebgp-requires-policy. By default, ebgp-requires-policy is enabled.

Usage Guidelines

Consider creating appropriate route maps and using them rather than disabling the policy check, as using policies is a more secure behavior, and can prevent unintended routes from being exchanged. Function ebgp-requires-policy is introduced and enabled by default.

With this command enable, EBGP will not exchange routes with a neighbor unless there is a route map configured on the address family neighbor entry which matches and permits the routes inbound and outbound. That is, without the incoming filter, no routes will be accepted; without the outgoing filter, no routes will be announced.

NOTE:

- If you do not want to control the route exchanging via use BGP policies, you need to disable this feature manually, or the route cannot be correctly exchanged.
- When ebgp-requires-policy is enabled but the incoming or outgoing filter is missing, the route cannot be correctly updated, additionally a **run show bgp neighbor** command would indicate in the *For address family*: block that:

```
admin@Xorplus# run show bgp neighbor
...
For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
...
For address family: IPv6 Unicast
  Update group 2, subgroup 2
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
```

Example

- Configure a BGP route policy "rm1" and enable ebgp-requires-policy to filter the incoming routes by using this policy.

```
admin@Xorplus# set routing prefix-list ipv4-family plist1 permit prefix 13.13.13.0/24
admin@Xorplus# set routing route-map rm1 order 1 matching-policy permit
admin@Xorplus# set routing route-map rm1 order 1 match ipv4-addr address prefix-list plist1
admin@Xorplus# set protocols bgp neighbor 192.168.170.1 ipv4-unicast in route-map rm1
admin@Xorplus# set protocols bgp ebgp-requires-policy true
admin@Xorplus# commit
```

set protocols bgp neighbor timers delayopen

The **set protocols bgp neighbor timers delayopen** command configures the timer to delay sending an OPEN message on a BGP connection. The delay allows the remote BGP Peer time to send the first OPEN message.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*>|**interface** <*interface*>**} timers delayopen** <*delayopen-timer*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the BGP.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an interface for BGP connection.
delayopen <*delayopen-timer*>	Specifies the time period to delay sending an OPEN message. The value is an integer, in seconds, that ranges from 1 to 240.

Example

- Configure the timer to delay sending an OPEN message on a BGP connection.

```
admin@Xorplus# set protocols bgp neighbor 192.168.170.2 timers delayopen 100
admin@Xorplus# commit
```

set protocols bgp neighbor maximum-prefix

The **set protocols bgp neighbor maximum-prefix** command sets a maximum number of prefixes we can receive from a given neighbor. If this number is exceeded, the BGP session will be destroyed.
The **delete protocols bgp neighbor maximum-prefix** command disables the maximum number of prefixes limit.

Command Syntax

set protocols bgp [**vrf** *<vrf-name>*] **neighbor** *<ip>* **ipv4-unicast maximum-prefix** *<max-prefix-number>*

delete protocols bgp [**vrf** *<vrf-name>*] **neighbor** *<ip>* **ipv4-unicast maximum-prefix** *<max-prefix-number>*

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** *<vrf-name>* [**description** *<string>*].
neighbor *<ip>*	Specifies the IPv4 address of a peer.
peer-group *<peer-group>*	Specifies a peer group.
interface *<interface>*	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
maximum-prefix *<max-prefix-number>*	Specifies the maximum number of prefixes allowed from the specified neighbor. The value is an integer from 1 to 4294967295. By default, there is no limit for the maximum number of prefixes.

Usage Guidelines

In practice, it is generally preferable to use a prefix-list to limit what prefixes are received from the peer instead of using this knob. Tearing down the BGP session when a limit is exceeded is far more destructive than merely rejecting undesired prefixes. The prefix-list method is also much more granular and offers much smarter matching criterion than number of received prefixes, making it more suited to implementing policy.

Example

• This example sets the prefix limit to 1000 prefixes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast maximum-prefix 1000
admin@XorPlus# commit
```

set protocols bgp neighbor maximum-prefix-out

The **set protocols bgp neighbor maximum-prefix-out** command sets a maximum number of prefixes we can send to a given neighbor. Since sent prefix count is managed by update-groups, this option creates a separate update-group for outgoing updates.
The **delete protocols bgp neighbor maximum-prefix-out** command disables the maximum number of prefixes limit.

Command Syntax

set protocols bgp [**vrf** *<vrf-name>*] **neighbor** *<ip>* **ipv4-unicast maximum-prefix-out** *<max-prefix-number>*

delete protocols bgp [**vrf** *<vrf-name>*] **neighbor** *<ip>* **ipv4-unicast maximum-prefix-out** *<max-prefix-number>*

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** *<vrf-name>* [**description** *<string>*].
neighbor *<ip>*	Specifies the IPv4 address of a peer.
peer-group *<peer-group>*	Specifies a peer group.
interface *<interface>*	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
maximum-prefix-out *<max-prefix-number>*	Specifies the maximum number of prefixes we can send to a given neighbor. The value is an integer from 1 to 4294967295. By default, there is no limit for the maximum number of prefixes.

Example
• This example sets the prefix limit we can send to a given neighbor to 1000 prefixes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast maximum-prefix-out 1000
admin@XorPlus# commit
```

set protocols bgp neighbor port

The **set protocols bgp neighbor port** command sets a custom TCP port of the neighbor on which to communicate with the BGP neighbor.
The **delete protocols bgp neighbor port** command allows a random TCP port to be selected for the communication with the BGP neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **port** <*port-number*>

delete protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **port** <*port-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
port <*port-number*>	Specifies a TCP port number. The value is an integer that ranges from 0 to 65535.

Example
• This example sets the TCP port of the neighbor to 1500.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 port 1500
admin@XorPlus# commit
```

set protocols bgp neighbor sender-as-path-loop-detection

The **set protocols bgp neighbor sender-as-path-loop-detection** command enables the detection of sender side AS path loops and filter the bad routes before they are sent. This setting is disabled by default.
The **delete protocols bgp neighbor sender-as-path-loop-detection** command removes the configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} sender-as-path-loop-detection**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} sender-as-path-loop-detection**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example enables the detection of sender side AS path loops and filter the bad routes before they are sent.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 sender-as-path-loop-detection
admin@XorPlus# commit
```

set protocols bgp fast-external-failover

The **set protocols bgp fast-external-failover** command can be used to set the switch to reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down.
The **delete protocols bgp fast-external-failover** command turns off this ability.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **fast-external-failover**

delete protocols bgp [***vrf*** <*vrf-name*>] **fast-external-failover**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example sets the switch to reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down.

```
admin@XorPlus# set protocols bgp fast-external-failover
admin@XorPlus# commit
```

set protocols bgp confederation identifier

The **set protocols bgp confederation identifier** command configures a BGP confederation with the confederation identifier. The group of Autonomous Systems (ASs) will be presented as a single autonomous system with the confederation identifier as the AS number.
The **delete protocols bgp confederation identifier** command deletes the BGP confederation identifier.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **confederation identifier** <*as-number*>

delete protocols bgp [***vrf*** <*vrf-name*>] **confederation identifier** <*as-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
identifier <*as-number*>	Specifies the identifier for the confederation. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example sets the BGP confederation with the AS number.

```
admin@XorPlus# set protocols bgp confederation identifier 55530
admin@XorPlus# commit
```

set protocols bgp confederation peers

The **set protocols bgp confederation peers** command configures BGP confederation peers with both same and different sub-autonomous system to establish an eBGP membership. The **delete protocols bgp confederation peers** command disables the peer session and deletes the peer information.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **confederation peers** <*as-number*>

delete protocols bgp [***vrf*** <*vrf-name*>] **confederation peers** <*as-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peers <*as-number*>	Specifies the autonomous system number to establish an eBGP membership. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example configures peers with ASNs.

```
admin@XorPlus# set protocols bgp confederation peers 62341
admin@XorPlus# commit
```

set protocols bgp dampening

The **set protocols bgp ipv4-unicast dampening** command enables (with optionally specified dampening parameters) or disables route-flap dampening for all routes of a BGP instance.
The **delete protocols bgp ipv4-unicast dampening** command deletes the configuration.

Command Syntax

set protocol bgp ipv4-unicast dampening [half-life-timer *<half-timer>* | **maximum-duration** *<max-duration>* | **start-reusing** *<lower-threshold>* | **start-suppressing** *<high-threshold>*]

delete protocols bgp ipv4-unicast dampening half-life-timer [half-life-timer *<half-timer>* | **maximum-duration** *<max-duration>* | **start-reusing** *<lower-threshold>* | **start-suppressing** *<high-threshold>*]

Parameter

Parameter	Description
half-life-timer *<half-timer>*	Optional. Specifies the half-life time in minutes. When the time expires, the penalty on a route gets reduced exponentially to half its current value. The value is an integer that ranges from 1 to 45. The default value is 15 minutes.
maximum-duration *<max-duration>*	Optional. Specifies the maximum duration to suppress a stable route in minutes. The value is an integer that ranges from 1 to 255. The default value is 60 minutes.
start-reusing *<lower-threshold>*	Optional. Specifies the lower threshold of penalty. On a suppressed route, when the penalty on a route falls below this value, the route is unsuppressed. The value is an integer that ranges from 1 to 20000. The default value is 750.
start-suppressing *<high-threshold>*	Optional. Specifies the upper threshold of penalty. When the penalty on a flapping route exceeds this value, the route is suppressed. The value is an integer that ranges from 1 to 20000. The default value is 2000.

Usage Guidelines

The dampening algorithm assigns a penalty of 1000 to a flapping route every time the route gets withdrawn. The penalty values accumulate on the route every time it flaps. However, the penalty decays and is reduced
to half its value by the half-life time.
NOTE: This feature is not applicable on IBGP routes.

Example
• This example enables dampening with optionally specified parameters.

```
admin@XorPlus# set protocol bgp ipv4-unicast dampening half-life-timer 20
admin@XorPlus# set protocol bgp ipv4-unicast dampening start-reusing 850
admin@XorPlus# set protocol bgp ipv4-unicast dampening start-suppressing 2500
admin@XorPlus# set protocol bgp ipv4-unicast dampening 30
admin@XorPlus# commit
```

set protocols bgp default local-preference

The **set protocols bgp default local-preference** command defaults local preference value for BGP learned routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.
The **delete protocols bgp default local-preference** command sets the local preference to the default value of 100.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **default local-preference** <*preference-value*>

delete protocols bgp [***vrf*** <*vrf-name*>] **default local-preference** <*preference-value*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
local-preference <*preference-value*>	Specifies the local preference value. The value is an integer that ranges from 0 to 4294967295. The default value is 100.

Example
• This example defaults local preference value for BGP learned routes to 20.

```
admin@XorPlus# set protocols bgp default local-preference 20
admin@XorPlus# commit
```

set protocols bgp as-notation

The **set protocols bgp as-notation** command configures the display format of the 4-byte Autonomous System (AS) numbers be shown for all show commands.

By default, the BGP 4-byte AS number is displayed in the same format as the AS number configured in the **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*> command.

The **delete protocols bgp as-notation** command deletes the configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **as-notation** <**dot | dot+ | plain**>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
dot	Specifies that Autonomous System (AS) numbers greater than 65535 be shown in dotted integer format for all show commands.
dot+	Specifies to force all Autonomous System (AS) numbers to be shown in dotted integer format for all show commands.
plain	Specifies that Autonomous System (AS) numbers be shown in non-dotted, simple integer.

Usage Guidelines

The **set protocols bgp as-notation** command changes the display format of the 4-byte AS number and AS_PATH that appears in the display information of all show commands.

The conversion relationship between 4-byte AS number in integer format (z) and 4-byte AS number in dotted format (x.y) is: z = x * 65536 + y, for example, a 4-byte AS number 10.2 in dotted format, the corresponding 4-byte AS number in integer format is: 10*65536+2=655362.

NOTE :

The **set protocols bgp as-notation** command and the **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*> command must be in the same commit. If you want to configure **as-notation** when the **local-as** configuration has been successfully committed, then you have to remove all the BGP configuration (all **set protocols bgp** xx commands) and then reconfigure to make sure that the **as-notation** command and the **local-as** command are in the same commit.

Example

- Configure the display format of the 4-byte Autonomous System (AS) numbers be shown in dotted integer format for all show commands.

```
admin@PICOS# set protocols bgp local-as 12
admin@PICOS# set protocols bgp as-notation dot+
admin@PICOS# commit
```

set protocols bgp neighbor local-as

The **set protocols bgp neighbor local-as** command configures an alternate local AS number that can be used to establish a session with a peer, allowing a router to appear to be a member of a second autonomous system (AS), and its real AS.

Local AS allows two autonomous systems to merge without modifying peering arrangements. This command is valid only for eBGP peers.

The **delete protocols bgp neighbor local-as** command restores the default, which is for a peering session to be established using the primary AS (primary AS is the real AS number specified at the time of neighbor creation using the command **set protocols bgp local-as**).

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**|peer-group** <*peer-group*>|**interface** <*interface*>**} local-as** <*AS-NUMBER*> [**no-prepend** [**replace-as**]]

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**|peer-group** <*peer-group*>|**interface** <*interface*>**} local-as**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
local-as <*AS-NUMBER*>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.
no-prepend [**replace-as**]	Optional. Specifies that the alternate local AS number is not prepended to the AS_PATH in BGP routes. • If the **no-prepend** attribute is specified, then the supplied local-as is not prepended to the received AS_PATH. • If the **replace-as** attribute is specified, then only the supplied local-as is prepended to the AS_PATH when transmitting local-route updates to this peer. Note that replace-as can only be specified if no-prepend is.

Usage Guidelines

Specify an alternate AS for this BGP process when interacting with a specified peer. With no modifiers (**no-prepend** [**replace-as**]), the specified local-as is prepended to the received AS_PATH when receiving routing updates from the peer, and prepended to the outgoing AS_PATH (after the process local AS) when transmitting local routes to the peer.

NOTES：

- AS number configured by command **set protocols bgp neighbor local-as** cannot be the same as local AS number (configured by command **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>) or remote AS number of the specified peer.
- For a switch in a BGP confederation, AS number configured in command **set protocols bgp neighbor local-as** cannot be the same as the AS number (configured by command **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>) of any switch in the BGP confederation.

This command is commonly used in scenarios where carriers modify their network deployments. For example, when carrier A acquires carrier B, the AS of carrier B needs to be merged into the AS of carrier A as they are located in different ASes, that is, the AS number of the carrier B is modified to the AS number of carrier A. However, during the network consolidation process, BGP peers of the original carrier B located in other ASs may not expect or be inconvenient to modify the local BGP configuration immediately, which may result in a loss of connectivity with these peers.

To ensure successful network consolidation progress, you can set the original AS number of carrier B as an alternate local AS number on carrier B by using command **set protocols bgp neighbor local-as**, which allows carrier B to keep connection with other BGP peers using the alternate AS number.

Example

- Configure an alternate local AS number that can be used to establish a session with an eBGP peer.

```
admin@PICOS# set protocols bgp neighbor 100.1.1.134 local-as 200
admin@PICOS# commit
```

OSPFv2 Commands

- run clear ospf interface
- run show ospf border-routers
- run show ospf database
- run show ospf interface
- run show ospf neighbor
- run show ospf route
- run show ospf summary-address
- set protocols ospf aggregation timer
- set protocols ospf area area-type
- set protocols ospf area filter-list prefix
- set protocols ospf area no-summary
- set protocols ospf area range
- set protocols ospf area virtual-link
- set protocols ospf area virtual-link authentication
- set protocols ospf area virtual-link authentication-key
- set protocols ospf area virtual-link dead-interval
- set protocols ospf area virtual-link hello-interval
- set protocols ospf area virtual-link message-digest-key md5
- set protocols ospf area virtual-link retransmit-interval
- set protocols ospf area virtual-link transmit-delay
- set protocols ospf auto-cost reference-bandwidth
- set protocols ospf compatible rfc1583
- set protocols ospf default-information originate
- set protocols ospf default-metric
- set protocols ospf interface area
- set protocols ospf interface authentication address
- set protocols ospf interface authentication message-digest
- set protocols ospf interface cost
- set protocols ospf interface dead-interval
- set protocols ospf interface hello-interval
- set protocols ospf interface message-digest-key md5
- set protocols ospf interface network
- set protocols ospf interface priority
- set protocols ospf interface retransmit-interval
- set protocols ospf interface transmit-delay
- set protocols ospf log-adjacency-changes
- set protocols ospf max-metric router-lsa administrative
- set protocols ospf max-metric router-lsa on-shutdown
- set protocols ospf max-metric router-lsa on-startup
- set protocols ospf multi-instance disable
- set protocols ospf network area
- set protocols ospf passive-interface
- set protocols ospf redistribute
- set protocols ospf redistribute metric-type
- set protocols ospf redistribute route-map
- set protocols ospf router-id
- set protocols ospf summary-address
- set protocols ospf timers lsa min-arrival
- set protocols ospf timers throttle spf
- set protocols ospf traceoption ism
- set protocols ospf traceoption lsa
- set protocols ospf traceoption nsm
- set protocols ospf traceoption packet
- set protocols ospf traceoption zebra
- set protocols ospf graceful-restart enable
- set protocols ospf capability opaque
- set protocols ospf graceful-restart grace-period
- set protocols ospf graceful-restart helper enable
- set protocols ospf graceful-restart helper planned-only
- set protocols ospf graceful-restart helper strict-lsa-checking
- set protocols ospf graceful-restart helper supported-grace-time
- run graceful-restart prepare ospf
- run show ospf graceful-restart helper

- set protocols ospf interface authentication-key

run clear ospf interface

Run the command **clear ospf interface** to clear or reset adjacency with the neighbor session. The specified interface should be a layer 3 interface.

Command Syntax

run clear ospf interface *<l3-interface>*

Parameter

Parameter	Description
interface *<l3-interface>*	Specifies the layer 3 interface. The value is a string.

Example

- Clear OSPF interface *vlan100*.

```
admin@XorPlus# run clear ospf interface vlan100
admin@Xorplus# commit
```

run show ospf border-routers

Run the command **run show ospf border-routers** to display OSPF ABRs and ASBRs.

If OSPF is running in multiple instance then add the instance ID parameter to the command to display ABRs and ASBRs within a particular OSPF instance.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf<***vrf-name***>] border-routers**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display ABRs and ASBRs in OSPF instance ID 1.

```
admin@switch1# run show ospf instance-id 1 border-routers
OSPF Instance: 1
============ OSPF router routing table =============
R    3.3.3.3               [10] area: 1.1.1.1, ASBR
                           via 11.251.201.4, vlan11
```

run show ospf database

To display the OSPF database, run the command **run show ospf database.** To display OSPF database summary, add the argument **summary** to the command.

If OSPF is running in multiple VRFs then add the parameter VRF to display OSPF database for the specified VRF. If multi-instance OSPF is running then add the instance ID to check the OSPF database for that instance.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf**<*vrf-name*>**] database [summary]**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name*>	Optional. Specifies the VRF name, the value is a string.

Example

- Display the OSPF database for vrf1.

```
admin@switch1# run show ospf vrf vrf1 database
VRF Name: vrf1

       OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          328 0x80000017 0xf095 1
2.2.2.2         2.2.2.2          405 0x80000018 0xadcf 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.251.201.3    2.2.2.2          345 0x80000014 0x89d6

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
11.251.201.0    1.1.1.1          388 0x80000014 0x80ea 11.251.201.0/24

                ASBR-Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
3.3.3.3         1.1.1.1          908 0x80000010 0xfa38

                Router Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1058 0x8000001a 0x0779 1
3.3.3.3         3.3.3.3         1087 0x8000001b 0x8be0 1

                Net Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum
11.251.201.4    3.3.3.3         1067 0x80000014 0x86cf

                Summary Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
10.251.201.0    1.1.1.1          378 0x80000014 0x8dde 10.251.201.0/24

                AS External Link States
```

```
Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         3.3.3.3         1607 0x80000010 0x7442 E2 0.0.0.0/0 [0x0]
```

To display OSPF database of an OSPF instance, run the command below

```
admin@Xorplus# run show ospf instance-id 1 database
OSPF Instance: 1

       OSPF Router with ID (41.41.41.41)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
41.41.41.41     41.41.41.41      119 0x80000003 0x3454 1

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.1.0     41.41.41.41      159 0x80000001 0x4004 192.168.1.0/24

                Router Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
41.41.41.41     41.41.41.41      119 0x80000003 0xd9b8 1

                Summary Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.11.0    41.41.41.41      159 0x80000001 0xd168 192.168.11.0/24
```

run show ospf interface

Run the command **run show ospf interface** to display information about layer 3 interfaces participating in OSPF process. The command output displays information such as interface name, IP address, the area this interfaces belongs to, neighbor adjacency count, multicast group memberships and OSPF timers etc.

To display the interface traffic related to OSPF, add the argument **traffic** to the command. This will display information such as OSPF hello messages sent and received on the interface, database description messages sent and received etc. You can also specify a particular interface to show information related to that L3 interface.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf<***vrf-name***>] interface** [**traffic | an-interface** <*vlan-interface*>]

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the name of the VRF. The value is a string.
interface<traffic>	Show traffic related to OSPF interfaces.
an-interface <*vlan-interface*>	Specify a L3 interface, the value is a string. It can be the VLAN interface name, the routed interface or the sub-interface name.

Example

- Show OSPF interface related information in OSPF instance ID 1.

```
admin@Xorplus# run show ospf instance-id 1 interface
OSPF Instance: 1

vlan111 is up
  ifindex 257, MTU 1500 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
  Internet Address 192.168.1.11/24, Broadcast 192.168.1.255, Area 1.1.1.1
  MTU mismatch detection: enabled
  Router ID 41.41.41.41, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  No backup designated router on this network
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 8.646s
  Neighbor Count is 1, Adjacent neighbor count is 0
vlan1111 is up
  ifindex 265, MTU 1500 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
  Internet Address 192.168.11.2/24, Broadcast 192.168.11.255, Area 0.0.0.0
  MTU mismatch detection: enabled
  Router ID 41.41.41.41, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  No backup designated router on this network
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 3.016s
  Neighbor Count is 1, Adjacent neighbor count is 0
```

run show ospf neighbor

Run the command **run show ospf neighbor** to display the OSPF neighbor devices. The command output displays the neighbor router ID, State, Dead Time, Address and Interface etc.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

If you require more detail about OSPF neighbors then add the argument **detail** to the command which will display information about the OSPF area the neighbor belongs to and recent state change statistics etc.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] neighbor [detail]**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Specifies the VLAN interface name.

Example

- The command below displays OSPF neighbors (two) for switch1 in vrf1.

```
admin@switch1# run show ospf vrf vrf1 neighbor
VRF Name: vrf1

Neighbor ID     Pri State           Dead Time Address         Interface                       RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR           38.590s 10.251.201.3    vlan10:10.251.201.2                 0     0     0
3.3.3.3           1 Full/DR           30.605s 11.251.201.4    vlan11:11.251.201.2                 0     0     0


admin@switch1# run show ospf vrf vrf1 neighbor detail
VRF Name: vrf1
 Neighbor 2.2.2.2, interface address 10.251.201.3
    In the area 0.0.0.0 via interface vlan10
    Neighbor priority is 1, State is Full, 6 state changes
    Most recent state change statistics:
      Progressive change 57m32s ago
    DR is 10.251.201.3, BDR is 10.251.201.2
    Options 2 *|-|-|-|-|-|E|-
    Dead timer due in 37.160s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on

 Neighbor 3.3.3.3, interface address 11.251.201.4
    In the area 1.1.1.1 via interface vlan11
    Neighbor priority is 1, State is Full, 6 state changes
    Most recent state change statistics:
      Progressive change 57m30s ago
    DR is 11.251.201.4, BDR is 11.251.201.2
    Options 2 *|-|-|-|-|-|E|-
    Dead timer due in 39.177s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on

To see the OSPF neighbors in an OSPF instance, run the command below

admin@Xorplus# run show ospf instance-id 1 neighbor
OSPF Instance: 1


Neighbor ID     Pri State           Dead Time Address         Interface                       RXmtL RqstL DBsmL
81.81.81.81       1 Init/DROther      36.580s 192.168.1.12    vlan111:192.168.1.11                0     0     0
171.171.171.171   1 Init/DROther      35.310s 192.168.11.1    vlan1111:192.168.11.2               0     0     0
```

run show ospf route

Run the command **run show ospf route** to display OSPF routes in the routing table.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Add the optional parameter **instance-id** to show routes of a specific OSPF instance in the default VRF.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] route**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the VRF name. The value is a string.

Example

- Display OSPF routes of switch1 in vrf1.

```
admin@switch1# run show ospf vrf vrf1 route
VRF Name: vrf1
============ OSPF network routing table ============
N    10.251.201.0/24       [10] area: 0.0.0.0
                           directly attached to vlan10
N    11.251.201.0/24       [10] area: 1.1.1.1
                           directly attached to vlan11

============ OSPF router routing table =============
R    3.3.3.3               [10] area: 1.1.1.1, ASBR
                           via 11.251.201.4, vlan11

============ OSPF external routing table ===========
N E2 0.0.0.0/0             [10/1] tag: 0
                           via 11.251.201.4, vlan11



admin@Xorplus# run show ospf instance-id 1 route
OSPF Instance: 1

============ OSPF network routing table ============
N    192.168.1.0/24        [10] area: 1.1.1.1
                           directly attached to vlan111
N    192.168.11.0/24       [10] area: 0.0.0.0
                           directly attached to vlan1111
```

run show ospf summary-address

The **run show ospf summary-address** command shows the configuration for display all configured summary routes with matching external LSA information.

Command Syntax

run show ospf summary-address [detail]

Parameters

Parameter	Description
detail	Optional. Shows a detailed view of all configured summary routes with matching external LSA information.

Example

- The following commands shows the configuration for display all configured summary routes with matching external LSA information.

```
admin@Xorplus# run show ospf summary-address
Summary-address     Metric-type     Metric     Tag         External_Rt_count
aggregation delay interval :100(in seconds)
10.10.0.0/16          E2            20         1234        0
```

set protocols ospf aggregation timer

The **set protocols ospf aggregation timer** command configures ASBR route summarization delay timer interval. Summarization starts only after this delay timer expiry.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] aggregation timer** <*aggregation-timer*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
Aggregation timer <*aggregation-timer*>	Specifies delay timer for starting ASBR route summarization. The value is an integer that ranges from 5 to 1800, in seconds. The default value is 5 seconds.

Example

- The following commands changes the ASBR route summarization delay timer to 100 seconds.

```
admin@Xorplus# set protocols ospf aggregation timer 100
admin@Xorplus# commit
```

set protocols ospf area area-type

Run the command **set protocols ospf area area-type** to define an OSPF area type. Two types of areas can be specified here. To create a stub area, choose the key word **stub**, or choose **nssa**, to create OSPF *not-so-stubby-area.* Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf area stub** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf**<*vrf-name*>**] area {**<*ipv4*>**|**<*area-id*>**} area-type <stub|nssa>**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>**|**<*area-id*>**} area-type <stub|nssa>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specify OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
stub	Keyword to specify a stub area.
nssa	Keyword to specify a not-so-stubby-area.

Example

- Configure area 1.1.1.1 in the default VRF as a stub area.

```
admin@XorPlus# set protocols ospf instance-id 1 area 1.1.1.1 area-type stub
admin@Xorplus# commit
```

set protocols ospf area filter-list prefix

Run the command **set protocols ospf area filter-list prefix** to create a filter list which acts as an access list for route advertisement in OSPF. This command filters Type-3 summary-LSAs to or from area using prefix lists. Keywords **in** or **out** is used to specify the inbound or outbound direction for the filter list. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf area filter-list prefix** to delete this configuration.

Command Syntax.

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} {in|out} filter-list prefix** <*prefix-list-v4*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} {in|out} filter-list prefix** <*prefix-list-v4*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
prefix <*prefix-list*>	Specifies the filter list name.
in	Specifies the inbound direction.
out	Specifies the outbound direction.

Example

- Configure prefix list1 for VRF BLUE, area 1.1.1.1 in the outbound direction.

```
admin@XorPlus# set protocols ospf vrf BLUE area 1.1.1.1 out prefix-list prefix list1
admin@Xorplus# commit
```

set protocols ospf area no-summary

Run the command **set protocols ospf area** to define an OSPF area and disallow injecting inter-area routes. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. The keyword **no-summary** is used to disable injecting inter-area summaries into the specified stub area. The **no-summary** option makes the area totally stubby.

> Multi-Instance OSPF is only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf area** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] area {**<*ipv4*>**|**<*area-id*>**} no-summary**

delete protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] area {**<*ipv4*>**|**<*area-id*>**} no-summary**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
no-summary	Keyword to disable injecting inter-area summaries into the specified stub area.

Example

- Configure area 1.1.1.1 in for instance ID 1 in the default VRF and disable injecting inter-area summaries into this area.

```
admin@XorPlus# set protocols ospf instance-id 1 area 1.1.1.1 no-summary
admin@Xorplus# commit
```

set protocols ospf area range

The **set protocols ospf area range** command summarizes intra area paths from specified area into a single Type-3 summary-LSA announced to other areas. This command can be used only on ABR and ONLY router-LSAs (Type-1) and network-LSAs (Type-2, i.e. LSAs with scope area) can be summarized.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} range** <*prefix/mask*> [**advertise** <**true | false**> **| cost** <*cost*> **| substitute** <*prefix/mask*>]

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be in IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
range <*prefix/mask*>	Specifies summarizing routes matching the area range *prefix/mask*.
advertise <true | false>	Optional. Determines whether to advertise the summarized route or not. The value could be **true** or **false**. • **true**: Advertise the summarized route. • **false**: Do not advertise the summarized route. By default, the summarized route is advertised.
cost <*cost*>	Optional. Specifies the cost of the summarized route. The value is an integer that ranges from 0 to 16777215.
substitute <*prefix/mask* >	Optional. Specifies another prefix to substitute the already configured one to announce to other areas.

Example

- The following commands configure route summarization in OSPF area 1.

```
admin@Xorplus# set protocols ospf area 1 range 10.42.0.0/16
admin@Xorplus# commit
```

set protocols ospf area virtual-link

The **set protocols ospf area virtual-link** command creates an OSPF virtual link with a remote ABR and enters the vlink context.

The **delete protocols ospf area virtual-link** command deletes an OSPF virtual link with the specified router ID of the remote ABR. If no *<ROUTER-ID>* is specified, the command sets the virtual link to the default settings.

Command Syntax

set protocols ospf [**vrf** *<vrf-name>*] **area {***<ipv4>*|*<area-id>***} virtual-link** *<ROUTER-ID>*

Parameters

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies the name of the VRF for the OSPF instance.
area {*<ipv4>*|*<area-id>*}	Specifies the OSPF area ID. The value could be in IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link *<ROUTER-ID>*	Configures a virtual link with the specified router ID of the remote ABR.

Example

- Configuring OSPF virtual links:

```
admin@Xorplus# set protocols ospf area 1 virtual-link 100.0.1.1
admin@Xorplus# commit
```

set protocols ospf area virtual-link authentication

Run the command **set protocols ospf area virtual-link authentication** to set the OSPF virtual-link authentication type that will be used for authentication with the remote ABR.

The command **delete protocols ospf area virtual-link authentication** unconfigures the virtual-link authentication type used and sets it to Null authentication, means no authentication.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication** [<**message-digest | null**>]

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication** [<**message-digest | null**>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
authentication [<**message-digest	null**>]	Choose one of the authentication types from the following parameters. • **message-digest:** Optional. Sets the authentication type to message-digest. • **null**: Optional. Sets the authentication type to null, means no authentication. If no authentication types is specified, the simple-text authentication type will be used.

Usage Guidelines

The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

When authentication type **message-digest** is configured, command set protocols ospf area virtual-link message-digest-key md5 can be used to set the md5 password.

When using **simple-text** authentication type, command set protocols ospf area virtual-link authentication-key can be used to set the password.

Example

- Configure OSPF virtual links authentication type:

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 authentication message-digest
admin@Xorplus# commit
```

set protocols ospf area virtual-link authentication-key

Run the command **set protocols ospf area virtual-link authentication-key** to set the OSPF virtual-link authentication password that is used for simple-text authentication.

The command **delete protocols ospf area virtual-link authentication-key** deletes the virtual-link authentication password that is used for simple-text authentication.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication-key** <*PASSWORD*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication-key**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
authentication-key <*PASSWORD*>	Specifies the password for simple-text authentication. The value is a string of 6 to 8 characters.

Example

- Configure OSPF virtual links authentication password:

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 authentication-key afsjlfk
admin@Xorplus# commit
```

set protocols ospf area virtual-link dead-interval

Run the command **set protocols ospf area virtual-link dead-interval** to configure the OSPF neighbor router of a virtual link dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf area virtual-link dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **dead-interval** <*seconds*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **dead-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
dead-interval <*seconds*>	Specifies the OSPF neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPF neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf area virtual-link hello-interval

Run the command **set protocols ospf area virtual-link hello-interval** to set the OSPF hello interval on the virtual link. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf area virtual-link hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **hello-interval** <*seconds*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **hello-interval** <*seconds*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
hello-interval <*seconds*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on the virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf area virtual-link message-digest-key md5

Run the command **set protocols ospf area virtual-link message-digest-key md5** to set OSPF authentication key to a cryptographic password. The cryptographic algorithm is MD5. The key number can be any digit between 1 and 255.

Note: Its important to configure the same key number and password on both ends for the OSPF authentication to be successful.

To delete the configuration, run the command **delete protocols ospf area virtual-link message-digest-key md5**.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **message-digest-key** <*1-255*> **md5** <*password*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **message-digest-key** <*1-255*> **md5** <*password*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
message-digest-key <*1-255*>	Specifies the MD5 key ID. The value is an integer in the range of 1 to 255.
md5 <*password*>	Specifies the MD5 authentication password that is used for message-digest authentication. The value is a string of 6 to 16 characters.

Usage Guidelines

The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

PicOS recommends you configure only one set of **message-digest-key** and **md5** password.

Example

- Configure MD5 key ID as 1.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 message-digest-key 1 md5 wrwgdygd
admin@Xorplus# commit
```

set protocols ospf area virtual-link retransmit-interval

Run the command **set protocols ospf area virtual-link retransmit-interval** to set the time between retransmitting lost link state advertisements for the OSPF virtual link.
The command **delete protocols ospf area virtual-link retransmit-interval** sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPF virtual link.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **retransmit-interval** <*INTERVAL*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **retransmit-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
retransmit-interval <*INTERVAL*>	Specifies the retransmit interval, in seconds. Range: 1 to 65535. Default: 5.

Example

- Configure the OSPF retransmit interval for the OSPF virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 retransmit-interval 30
admin@Xorplus# commit
```

set protocols ospf area virtual-link transmit-delay

Run the command **set protocols ospf area virtual-link transmit-delay** to set the time delay in link state transmission for the OSPF virtual link.
The command **delete protocols ospf area virtual-link transmit-delay** sets the delay in link state transmission to the default of 1 second for the OSPF virtual link.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **transmit-delay** <*DELAY*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **transmit-delay**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
transmit-delay <*DELAY*>	Specifies the transit delay in seconds. Range: 1 to 65535. Default: 1.

Example

- Configure the OSPF transmit delay on the virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 transmit-delay 30
admin@Xorplus# commit
```

set protocols ospf auto-cost reference-bandwidth

Run the command **set protocols ospf auto-cost reference-bandwidth** to set the reference bandwidth for automatic route cost calculation. The reference bandwidth specified here is considered equivalent to OSPF cost of 1. The default bandwidth is 100Mbits/s, that is, a link with bandwidth of 100Mbits/s or higher is considered to have a cost of 1. Cost of links with lower bandwidth will be calculated with reference to this bandwidth value. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional parameter **vrf** can be used to specify the name of the VRF for the OSPF instance.

Note that this configuration must be consistent within the OSPF domain.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf auto-cost reference-bandwidth** to delete this configuration

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] auto-cost reference-bandwidth** <*ref-bandwidth*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] auto-cost reference-bandwidth** <*ref-bandwidth*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
reference-bandwidth <*ref-bandwidth*>	Specifies the reference bandwidth. The value is an integer that ranges from 1 to 4294967.

Example

- Configure the OSPF reference bandwidth to 500000 for the default VRF OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 auto-cost reference-bandwidth 500000
admin@Xorplus# commit
```

set protocols ospf compatible rfc1583

Run the command **set protocols ospf compatible rfc1583** to enable OSPF compatibility with RFC1583 (backward compatibility). If RFC1583 compatibility is enabled, then the route cost calculation follows a different method.

Run the command **delete protocols ospf compatible** to delete this configuration.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] compatible rfc1583**

delete protocols ospf [vrf <*vrf-name*>**] compatible**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable OSPF RFC1583 compatibility:

```
admin@XorPlus# set protocols ospf vrf BLUE compatible rfc1583
admin@Xorplus# commit
```

set protocols ospf default-information originate

Run the command **set protocol ospf default-information originate** to originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional keyword **vrf** specifies the name of the VRF for the OSPF instance. If the optional keyword **always** is given then the default route is always advertised, even when there is no default route present in the routing table.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocol ospf default-information originate** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf <***vrf-name***>] default-information originate [always]**

delete protocols ospf [instance-id <*instance-id***> | vrf <***vrf-name***>] default-information originate [always]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
always	Optional keyword that specifies that the default route is always advertised regardless if its present in the routing table.

Example

- Configure the device to always originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas.

```
admin@XorPlus# set protocols ospf instance-id 1 default-information originate always
admin@Xorplus# commit
```

set protocols ospf default-metric

Run the command **set protocols ospf default-metric** to set the default metric for redistributed routes in the OSPF.
The command **delete protocols ospf default-metric** sets the default metric to be used for redistributed routes into OSPF to the default of 20.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **default-metric** <*METRIC-VALUE*>

delete protocols ospf [**vrf** <*vrf-name*>] **default-metric**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
default-metric <*METRIC-VALUE*>	Specifies the default metric value to use for redistributed routes. The value could be an integer that ranges from 0 to 1677214. The default value is 20.

Example

- Configure default metric for redistributed routes:

```
admin@XorPlus# set protocols ospf default-metric 37
admin@Xorplus# commit
```

set protocols ospf interface area

To enable OSPF on an interface and assign the interface to an area, use the **set protocols ospf interface area** command in L2/L3 configuration mode. The interface will send and accept OSPF LSAs (link-state advertisements). Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

Run the command **delete protocols ospf interface area** to remove this configuration from the system.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] interface** <*interface-name*> **area {**<*ipv4*>|<*area-id*>**}**

delete protocols ospf [instance-id <*instance-id***>] interface** <*interface-name*> **area {**<*ipv4*>|<*area-id*>**}**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
area {<*ipv4*>|<*area-id*>**}**	Specifies the OSPF area in IPv4 format or an integer in the range of 0 to 4294967295.

Usage Guidelines

The OSPF commands **set protocols ospf interface area** and **set protocols ospf network area** cannot be configured simultaneously. The user can enable OSPF for either an interface or netowrk, but not both. If one of the two commands has been configured on the device and the user tries to commit the different method of enabling OSPF will result in commit failed error message.

The user must delete the configuration method previously committed before trying to commit the different method and keep the following points in mind:

- If **set protocols ospf network area** has been configured on the device first, you have to delete it before configuring command **set protocols ospf interface area**.
- If **set protocols ospf interface area** has been configured on the device first, and if the configuration is in a specified VRF, you have to delete all OSPF configurations under the specified VRF before configuring the command **set protocols ospf vrf network area**. Or if these configurations are in the default VRF, you have to delete all OSPF configurations of ***all*** VRFs on the device by using command **delete protocols ospf** before configuring **set protocols ospf network area**.

Example

- Enable OSPF on interface vlan200 and assign it to area 1.1.1.1 for instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 interface vlan200 area 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf interface authentication address

Run the command **set protocols ospf interface authentication address** to set the authentication address that is used for OSPF authentication. This command is a mandatory configuration for OSPF authentication.
The command **delete protocols ospf interface authentication address** deletes the authentication address that is used for OSPF authentication.

Command Syntax

set protocols ospf interface <*interface-name*> **authentication address** <*ipv4*>

delete protocols ospf interface <*interface-name*> **authentication address**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
authentication address <*ipv4*>	Specifies the IPv4 address of the interface.

Example

- Configure the authentication address that is used for OSPF authentication.

```
admin@XorPlus# set protocols ospf interface vlan200 authentication address 10.10.114.1
admin@Xorplus# commit
```

set protocols ospf interface authentication message-digest

Run the command **set protocols ospf interface authentication message-digest** to specify that OSPF packets must be authenticated with MD5 HMACs on the given interface.

Note that you must first create MD5 key using the command **set protocols ospf interface message-digest-key** <1-255> **md5** <key-string> before you can enable MD5 authentication on the interface.

Command Syntax

set protocols ospf interface <*interface-name*> **authentication message-digest**

delete protocols ospf interface <*interface-name*> **authentication message-digest**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- Enable MD5 authentication on interface vlan200.

```
admin@XorPlus# set protocols ospf interface vlan200 authentication message-digest
admin@Xorplus# commit
```

set protocols ospf interface cost

Run the command **set protocols ospf interface cost** to set the OSPF link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation. Changing the interface cost causes the OSPF to run the SPF and reissue LSAs.

Run the command **delete protocols ospf interface cost** to remove this configuration.

Command Syntax

set protocols ospf interface <*interface-name*> **cost** <*1-65535*>

delete protocols ospf interface <*interface-name*> **cost**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
cost <*1-65535*>	Specifies the link cost, the value is an integer in the range of 1 to 65535.

Example

- Configure the OSPF interface vlan200 cost to 5.

```
admin@XorPlus# set protocols ospf interface vlan200 cost 5
admin@Xorplus# commit
```

set protocols ospf interface dead-interval

Run the command **set protocols ospf interface dead-interval** to configure the OSPF neighbor router dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf interface dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **dead-interval** <*seconds*>

delete protocols ospf interface <*interface-name*> **dead-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dead-interval <*seconds*>	Specifies the OSPF neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPF neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf interface vlan200 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf interface hello-interval

Run the command **set protocols ospf interface hello-interval** to set the OSPF hello interval on the specified interface. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf interface hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **hello-interval** <*seconds*>

delete protocols ospf interface <*interface-name*> **hello-interval** <*seconds*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
hello-interval <*seconds*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on interface vlan200.

```
admin@XorPlus# set protocols ospf interface vlan200 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf interface message-digest-key md5

Run the command **set protocols ospf interface message-digest-key md5** to specify the MD5 key number and password for MD5 authentication for a given interface. The key number can be any digit between 1 and 255. The password string can be any string without spaces, the maximum length of the string should be 16 characters.

Note: Its important to configure the same key number and password on both ends for the OSPF authentication to be successful.

To delete the configuration, run the command **delete protocols ospf interface message-digest-key.**

Command Syntax

set protocols ospf interface <*interface-name*> **message-digest-key** <*1-255*> **md5** <*password*>

delete protocols ospf interface <*interface-name*> **message-digest-key** <*1-255*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
message-digest-key <*1-255*>	Specifies the MD5 key ID. The value is an integer in the range of 1 to 255
md5 <*text*>	Specifies the MD5 key string, the maximum length should not exceed 16 characters and should not have spaces.

Example

- Configure MD5 key ID as 1 and password string as testkey.

```
admin@XorPlus# set protocols ospf interface vlan200 message-digest-key 1 md5 testkey
admin@Xorplus# commit
```

set protocols ospf interface network

Run the command **set protocols ospf interface network** to enable OSPF on an interface and specify a network type. Enabling OSPF on an interface allows the interface to send and receive LSAs. Four different network types can be specified here namely, **broadcast, non-broadcast, point-to-multipoint** and **point-to-point**.

To delete this configuration, run the command **delete protocols ospf interface network**

Command Syntax

set protocols ospf interface <*interface-name*> **network <broadcast|non-broadcast|point-to-multipoint|point-to-point>**

delete protocols ospf interface <*interface-name*> **network <broadcast|non-broadcast|point-to-multipoint|point-to-point>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
broadcast	Specifies the OSPF broadcast multi-access network.
non-broadcast	Specifies the OSPF NBMA network.
point-to-multipoint	Specifies the OSPF point-to-multipoint network.
point-to-point	Specifies the OSPF point-to-point network.

Example

- Enable OSPF on interface vlan200 and specify network type as point-to-point.

```
admin@XorPlus# set protocols ospf interface vlan200 network point-to-point
admin@Xorplus# commit
```

set protocols ospf interface priority

Run the command **set protocols ospf interface priority** to set the OSPF priority for the interface. The larger the numeric value of the priority, the higher the chances for it to become the designated router. Setting a priority of zero makes the router ineligible to become a designated router or back up designated router.
The command **delete protocols ospf interface priority** sets the OSPF priority for the interface to the default of 1.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **priority** <*PRIORITY-VALUE*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **priority**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
priority <*PRIORITY-VALUE*>	Specifies the OSPF priority value. Range: 0 to 255. Default: 1.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF vlan200 priority to 5.

```
admin@XorPlus# set protocols ospf interface vlan200 priority 5
admin@Xorplus# commit
```

set protocols ospf interface retransmit-interval

Run the command **set protocols ospf interface retransmit-interval** to set the time between retransmitting lost link state advertisements for the OSPF interface.
The command **delete protocols ospf interface retransmit-interval** sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPF interface.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **retransmit-interval** <*INTERVAL*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **retransmit-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
retransmit-interval <*INTERVAL*>	Specifies the retransmit interval, in seconds. Range: 1 to 65535. Default: 5.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF retransmit interval on the interface.

```
admin@XorPlus# set protocols ospf interface vlan200 retransmit-interval 30
admin@Xorplus# commit
```

set protocols ospf interface transmit-delay

Run the command **set protocols ospf interface transmit-delay** to set the time delay in link state transmission for the OSPF interface.
The command **delete protocols ospf interface transmit-delay** sets the delay in link state transmission to the default of 1 second for the OSPF interface.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **transmit-delay** <*DELAY*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **transmit-delay**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
transmit-delay <*DELAY*>	Specifies the transit delay in seconds. Range: 1 to 65535. Default: 1.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF transmit delay on the interface.

```
admin@XorPlus# set protocols ospf interface vlan200 transmit-delay 30
admin@Xorplus# commit
```

set protocols ospf log-adjacency-changes

Run the command **set protocols ospf log-adjacency-changes** to log changes in OSPF adjacency state. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. Add the optional **detail** argument to log all changes in adjacency state. Without the **detail** keyword, only changes to full or regressions are logged. You can optionally specify the VRF for the single instance OSPF in the non-default VRF for this command to take effect.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf log-adjacency-changes** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] log-adjacency-changes [detail]**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] log-adjacency-changes [detail]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
detail	Optional. Specifies to log all changes in adjacency state.

Example

- Configure OSPF to log all adjacency changes for VRF BLUE.

```
admin@XorPlus# set protocols ospf vrf BLUE log-adjacency-changes detail
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa administrative

The **set protocols ospf max-metric router-lsa administrative** command configures the protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations.

Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period of time. The command will then take effect until manually deleted.

The **delete protocols ospf max-metric router-lsa administrative** command deletes the configuration.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**

delete protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative** is configured for advertising the maximum metric.

```
admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 0.539s ago
Last SPF duration 173 usecs
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
 Refresh timer 10 secs
Maximum multiple paths(ECMP) supported  256
This router is an ASBR (injecting external routing information)
Number of external LSA 5. Checksum Sum 0x000211ba
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
   Number of interfaces in this area: Total: 11, Active: 10
   Originating stub / maximum-distance Router-LSA
     Administratively activated (indefinitely)
```

Number of fully adjacent neighbors in this area: 1

Area has no authentication

SPF algorithm executed 40 times

Number of LSA 4

Number of router LSA 3. Checksum Sum 0x0001a0d5

Number of network LSA 1. Checksum Sum 0x000068d5

Number of summary LSA 0. Checksum Sum 0x00000000

Number of ASBR summary LSA 0. Checksum Sum 0x00000000

Number of NSSA LSA 0. Checksum Sum 0x00000000

Number of opaque link LSA 0. Checksum Sum 0x00000000

Number of opaque area LSA 0. Checksum Sum 0x00000000

Example

- Setting to maximize the cost metrics for Router LSA to administrative:

```
admin@Xorplus# set protocols ospf max-metric router-lsa administrative
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa on-shutdown

The **set protocols ospf max-metric router-lsa on-shutdown** command configures the protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations. **on-shutdown** *<advert-time>* indicates to advertise a maximum metric in advance of shutdown for the *advert-time* configured in seconds to gracefully excuse itself from the OSPF domain.

The **delete protocols ospf max-metric router-lsa on-shutdown** command advertises the normal cost metrics instead of advertising the maximized cost metric.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** *<vrf-name>*] **max-metric router-lsa on-startup** *<advert-time>*
>
> **set protocols ospf** [**vrf** *<vrf-name>*] **max-metric router-lsa on-shutdown** *<advert-time>*
>
> **set protocols ospf** [**vrf** *<vrf-name>*] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** *<vrf-name>*] **max-metric router-lsa on-shutdown** *<advert-time>*

delete protocols ospf [**vrf** *<vrf-name>*] **max-metric router-lsa on-shutdown**

Parameters

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** *<vrf-name>* [**description** *<string>*].
on-shutdown *<advert-time>*	Specifies the time interval to advertise a maximum metric in advance of shutdown. The value is an integer, in seconds, that ranges from 5 to 100.

Usage Guidelines

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** *<vrf-name>*] **max-metric router-lsa on-shutdown** *<advert-time>* is configured with 100 seconds, and 1 minutes 31 seconds remaining is left for advertising the maximum metric and shutting down the router.

```
admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Deferred shutdown in progress, 1m31s remaining
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Stub router advertisement is configured
  Enabled for 100s prior to full shutdown
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 8.551s ago
Last SPF duration 201 usecs
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
 Refresh timer 10 secs
Maximum multiple paths(ECMP) supported  256
This router is an ASBR (injecting external routing information)
Number of external LSA 2. Checksum Sum 0x0000d86e
```

```
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
  Number of interfaces in this area: Total: 11, Active: 10
  Originating stub / maximum-distance Router-LSA
  Administratively activated (indefinitely)
  Number of fully adjacent neighbors in this area: 2
  Area has no authentication
  SPF algorithm executed 8 times
  Number of LSA 6
  Number of router LSA 3. Checksum Sum 0x00013603
  Number of network LSA 3. Checksum Sum 0x0001509c
  Number of summary LSA 0. Checksum Sum 0x00000000
  Number of ASBR summary LSA 0. Checksum Sum 0x00000000
  Number of NSSA LSA 0. Checksum Sum 0x00000000
  Number of opaque link LSA 0. Checksum Sum 0x00000000
  Number of opaque area LSA 0. Checksum Sum 0x00000000
```

Example

- Setting to maximize the cost metrics for Router LSA on shutdown:

```
admin@Xorplus# set protocols ospf max-metric router-lsa on-shutdown 120
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa on-startup

The **set protocols ospf max-metric router-lsa on-startup** command configures the OSPF protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations. The parameter **on-startup** <*advert-time*> indicates to advertise a maximum metric from the time the OSPF neighbor is established for the *advert-time* configured in seconds.

The **delete protocols ospf max-metric router-lsa on-startup** command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>

delete protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
on-startup <*advert-time*>	Specifies the time interval to advertise a maximum metric from the time the OSPF neighbor is established. The value is an integer, in seconds, that ranges from 5 to 86400.

Usage Guidelines

This command is mainly used in the following scenarios:

1. When a new router is added to the OSPF network, but don't want to participate in data forwarding immediately. Then, **max-metric router-lsa on-startup** can be configured to establish the adjacency relationship and converge the network normally, while won't become an alternative path for other existing OSPF paths.
2. When a router is about to be disconnected from the network, to avoid neighbors from failing to detect it and causing a routing black hole, the **max-metric router-lsa on-shutdown** can be configured to enable the neighbors to recalculate the path before shutting down the router, and the data will no longer be forwarded through the router.

After the configuration **on-startup** <*advert-time*> is set, OSPF uses the maximum metric (65535) in the advertising LSA (Link State Advertisement) for the configured <*advert-time*> time when OSPF neighbor is established.

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*> is configured with 300 seconds, and 3 minutes 39 seconds remaining is left for advertising the maximum metric.

```
admin@Xorplus# set protocols ospf vrf x max-metric router-lsa on-startup 300
admin@Xorplus# commit


admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Stub router advertisement is configured
  Enabled for 300s after start-up
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 2
SPF algorithm last executed 1m06s ago
Last SPF duration 95 usecs
```

SPF timer is inactive

LSA minimum interval 5000 msecs

LSA minimum arrival 1000 msecs

Write Multiplier set to 20

Refresh timer 10 secs

Maximum multiple paths(ECMP) supported 256

This router is an ASBR (injecting external routing information)

Number of external LSA 2. Checksum Sum 0x0000fc5c

Number of opaque AS LSA 0. Checksum Sum 0x00000000

Number of areas attached to this router: 1

Area ID: 0.0.0.0 (Backbone)

Number of interfaces in this area: Total: 11, Active: 10

Originating stub / maximum-distance Router-LSA

Active from startup, 3m39s remaining

Number of fully adjacent neighbors in this area: 1

Area has no authentication

SPF algorithm executed 6 times

Number of LSA 5

Number of router LSA 3. Checksum Sum 0x00013649

Number of network LSA 2. Checksum Sum 0x0000f3a3

Number of summary LSA 0. Checksum Sum 0x00000000

Number of ASBR summary LSA 0. Checksum Sum 0x00000000

Number of NSSA LSA 0. Checksum Sum 0x00000000

Number of opaque link LSA 0. Checksum Sum 0x00000000

Number of opaque area LSA 0. Checksum Sum 0x00000000

Example

- Setting to maximize the cost metrics for Router LSA on startup:

```
admin@Xorplus# set protocols ospf max-metric router-lsa on-startup 300
admin@Xorplus# commit
```

set protocols ospf multi-instance disable

Run the command **set protocols ospf multi-instance disable** to enable or disable OSPF multi-instance mode.

Command Syntax

set protocols ospf multi-instance disable <true | false>

Example

- This example enables OSPF multi-instance on the device.

```
admin@XorPlus# set protocols ospf multi-instance disable false
admin@XorPlus# commit
```

set protocols ospf network area

Run the command **set protocols ospf network area** to configure OSPF instance for the IP subnet prefix with an area address per network. The optional parameter **vrf** can be used to specify OSFP instance for a particular VRF. If VRF is not defined then OSPF instance takes effect for the default VRF.

Run the command **delete protocols ospf network area** to delete this configuration.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] network** <*ipv4/prefixlen*> **area {**<*ipv4*|<*area-id*>**}**

delete protocols ospf [vrf <*vrf-name*>**] network** <*ipv4/prefixlen*> **area {**<*ipv4*>|<*area-id*>**}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
network <*ipv4/prefixlen*>	Specifies the network prefix and prefix length in IPv4 format.
area {<*ipv4*>|<*area-id*>**}**	Specify OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Usage Guidelines

The OSPF commands **set protocols ospf interface area** and **set protocols ospf network area** cannot be configured simultaneously. The user can enable OSPF for either an interface or netowrk, but not both. If one of the two commands has been configured on the device and the user tries to commit the different method of enabling OSPF will result in commit failed error message.

The user must delete the configuration method previously committed before trying to commit the different method and keep the following points in mind:

- If **set protocols ospf network area** has been configured on the device first, you have to delete it before configuring command **set protocols ospf interface area**.
- If **set protocols ospf interface area** has been configured on the device first, and if the configuration is in a specified VRF, you have to delete all OSPF configurations under the specified VRF before configuring the command **set protocols ospf vrf network area**. Or if these configurations are in the default VRF, you have to delete all OSPF configurations of ***all*** VRFs on the device by using command **delete protocols ospf** before configuring **set protocols ospf network area**.

Example

- Enable OSPF for network 10.0.0.0/16 in VRF BLUE and specify area 1.1.1.1.

```
admin@XorPlus# set protocols ospf vrf BLUE network 10.0.0.0/16 area 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf passive-interface

Run the command **set protocols ospf passive-interface** to the set the specified layer 3 interface as passive OSPF interface. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify the VRF for this command to take effect in, if not specified the command affects the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Passive interfaces are part of the OSPF database but they do not send or receive OSPF LSAs and hence OSPF adjacencies are not formed on these interfaces.

To delete the configuration, run the command **delete protocols ospf passive-interface.**

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] passive-interface** <*interface*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] passive-interface** <*interface*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
passive-interface <interface>	Specify a L3-interfaces to set to passive mode.

Example

- Set interface *vlan20* to OSPF passive mode for OSPF instance ID 1 in the default VRF.

```
admin@XorPlus# set protocols ospf instance-id 1 passive-interface vlan20
admin@Xorplus# commit
```

set protocols ospf redistribute

Run the command **set protocol ospf redistribute** to redistribute routes of a specified type or protocol into OSPF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF. You can optionally specify OSPF **metric** for the routes.

Run the command **delete protocol ospf redistribute** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|isis|rip|static|table** <*table-id*>**} [metric** <*metric*>**]**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|isis|rip|static|table** <*table-id*>**} [metric** <*metric*>**]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance. The value is a string.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
isis	Specify IS-IS routes for redistribution into OSPF.
rip	Specify RIP routes for redistribution into OSPF.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric <*metric*>	Optional. Specifies the route metric. The value is an integer that ranges from 0 to16777214.

Example

- Configure OSPF to redistribute BGP routes into OSPF in instance ID 1 with metric 5.

```
admin@XorPlus# set protocols ospf instance-id 1 redistribute bgp metric 5
admin@Xorplus# commit
```

set protocols ospf redistribute metric-type

Run the command **set protocols ospf redistribute metric-type** to specify metric type for OSPF route redistribution from other sources. There are two types of external routes, type 1 and type 2. A type 1 route has a metric that is the sum of the internal OSPF cost and the external redistributed cost. A type 2 route has a metric equal only to the redistributed cost. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional VRF can be specified for the single instance OSPF to configure the metric type.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf redistribute metric-type** to delete this configuration.

Command Syntax

set protocol ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table** <*table-id*>**} metric-type <1|2>**

delete protocol ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table|table** <*table-id*>} **metric-type <1|2>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the name of the VRF for the OSPF instance.
protocol bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric-type<1|2>	Specifies the OSPF external routes metric type. Metric type identifies how metric for the route is calculated.

Example

- Configure OSPF to redistribute BGP routes into OSPF with metric type 2.

```
admin@XorPlus# set protocols ospf instance-id 1 redistribute bgp metric-type 2
admin@Xorplus# commit
```

set protocols ospf redistribute route-map

Run the command **set protocols ospf redistribute route-map** to specify a route map to filter routes of different sources for redistribution into OSPF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf redistribute route-map** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf <***vrf-name***>] redistribute {bgp|connected|kernel|static|table <***table-id***>} route-map <***route-map***>**

delete protocols ospf [instance-id <*instance-id***> | vrf <***vrf-name***>] redistribute {bgp|connected|kernel|static|table <***table-id***>} route-map <***route-map***>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
route-map <*route-map*>	Specifies the route map to filter routes before redistributing them into OSPF.

Example

- Configure OSPF to redistribute BGP routes into OSPF and filter routes using route map map1 for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 vrf BLUE redistribute bgp route-map map1
admin@Xorplus# commit
```

set protocols ospf router-id

Run the command **set protocols ospf router-id** to configure OSPF router ID. The router ID should be unique within the OSPF domain and is in the IPv4 dotted decimal format. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf route-id** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] router-id** <*ipv4*>

delete protocols ospf [instance-id <*instance-id***>| vrf** <*vrf-name*>**] router-id** <*ipv4*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
router-id <*ipv4*>	Specify OSPF router ID. The value is in IPv4 dotted decimal format.

Example

- Configure OSPF router ID for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 router-id 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf summary-address

The **set protocols ospf summary-address** command summarizes the external routes with the matching address and mask. When advertising this route, its metric is set to the lowest cost path from among the routes that were summarized. This command can be used only on ASBR (Autonomous System Boundary Router).

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] summary-address** <*prefix/mask*> [**no-advertise | tag** <*tag-value*>]

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
summary-address <*prefix/mask*>	Specifies summarizing routes matching IPv4 address and mask *prefix/mask*.
no-advertise	Optional. Do not advertise the aggregate route. Suppress routes that match the specified prefix/mask pair.
tag <*tag-value*>	Optional. Specify the tag for the aggregate route. The summary prefix will be advertised along with the tag value in External LSAs. The value is an integer that ranges from 0 to 4294967295.

Example

- The following commands configure OSPF route summarization for ASBR.

```
admin@Xorplus# set protocols ospf summary-address 10.2.0.0/16 tag 2
admin@Xorplus# commit
```

set protocols ospf timers lsa min-arrival

Run the command **set protocols ospf timers lsa min-arrival** to set the minimum delay in receiving a new version of an LSA. The value of this parameter is in milliseconds and ranges from 0 to 600000. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify a VRF for the OSPF instance. If a VRF is not specified here, the command will affect OSPF for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf timers lsa min-arrival** to remove this configuration and go back to default delay of 1000 milliseconds.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] timers lsa min-arrival** <*milliseconds*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] timers lsa min-arrival** <*milliseconds*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the name of the VRF for the OSPF instance.
min-arrival <*milliseconds*>	Specify the minimum delay in receiving a new LSA in milliseconds. The value is an integer that ranges from 0 to 600000.

Example

- Configure OSPF minimum delay to receive LSA to 2000 milliseconds for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 timers lsa min-arrival 2000
admin@Xorplus# commit
```

set protocols ospf timers throttle spf

Run the command **set protocols ospf timers throttle spf** to set the *initial delay,* the *initial hold time* and the *maximum hold time* between when the SPF is calculated and the event which triggered the calculation. These timers prevent the system from overburdening the CPU with frequent SPF calculations. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify the name of the VRF for this configuration to take effect on. If the VRF name is not specified, the command takes effect on OSPF for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf timers throttle spf** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] timers throttle spf {delay**<*delay*> **| initial-holdtime**<*initial-hold-time*> **| maximum-holdtime**<*max-hold-time*>**}**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] timers throttle spf {**<*delay*> **|** <*initial-hold-time*> **|** <*max-hold-time*>**}**

Parameter

Parameter	Description
instance-id <*instance-id***>**	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
delay<*delay*>	Specifies the *initial delay*, the value ranges from 0 to 600000 milliseconds.
initial-holdtime<*initial-hold-time*>	Specifies the *initial hold time*, the value ranges from 0 to 600000 milliseconds.
maximum-holdtime<*max-hold-time*>	Specifies the *maximum hold time*, the value ranges from 0 to 600000 milliseconds.

Usage Guidelines

These three parameters are important fine tuning tools for OSPF. These timers are introduced to delay starting SFP calculations when a SPF-triggering event occurs. Frequent SPF calculations may incur heavy burden on the device resources such as CPU especially in large OSPF networks. The *delay* parameter specifies the delay in SPF calculation. This delay also applies to events occurring outside the *hold-time* of the previous SPF calculation. Two consecutive SPF calculations are always delayed by at least hold-time delay in milliseconds. The hold-time is initially set to the *initial hold-time* but its value is flexible and may be changed. If an event occurs within the hold-time of the previous SPF calculation, it results in increasing the hold-time by *initial hold-time.* If the flexible hold-time expires and no SPF triggering event occurs, the hold-time is reset to *initial hold-time.*

The example below sets the initial *delay* to 20ms, *initial hold-time* to 50ms and *maximum hold-time* to 5 seconds. This means that there will be a delay of 20ms between an SPF-triggering event and the commencement of the actual SPF calculation. The delay between two consecutive SPF calculations will be between 50ms and 5 seconds. If an SPF-triggering event occurs between the hold-time of the previous SPF calculation, the hold-time is increased by 50ms.

Example

- Configure OSPF SPF timers of initial delay time, minimum hold time and maximum hold time to 20, 50 and 5000ms respectively for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf delay 20
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf initial-holdtime 50
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf maximum-holdtime 5000
admin@Xorplus# commit
```

set protocols ospf traceoption ism

Run the command **set protocols ospf traceoption** to enable debugging for OSPF Interface State Machine (ISM). Optionally, you can choose to enable three different types of logging information, **status**, for ISM status information, **events**, for ISM events, or **timers** to get logging for timer s related information. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

Run the command **delete protocols ospf traceoption ism** to delete this information.

Command Syntax

set protocols ospf [instance-id <*instance-id*>] traceoption ism <status | events | timers>

delete protocols ospf [instance-id <*instance-id*>] traceoption ism <status | events | timers>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
ism <status | events | timers>	Specifies to enable ISM logging for either **status**, **events** or **timers**.

Example

- Enable OSPF ISM logging for status related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption ism status
admin@Xorplus# commit
```

set protocols ospf traceoption lsa

Run the command **set protocols ospf traceoption lsa** to enable logging of Link State Advertisement related messages. Three optional parameters, **generate, flooding, install,** or **refresh** can be used to specify logging for different types of LSA events. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption lsa** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption lsa <generate | flooding | install | refresh>**

delete protocols ospf [instance-id <*instance-id***>] traceoption lsa <generate | flooding | install | refresh>**

Parameter

Parameter	Description
instance-id <*instance-id***>**	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
lsa <generate | flooding | install | refresh>	Specifies to enable LSA logging for **generate, flooding, install** or **refresh** events.

Example

- Enable OSPF LSA logging for flooding related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption lsa flooding
admin@Xorplus# commit
```

set protocols ospf traceoption nsm

Run the command **set protocols ospf traceoption nsm** to enable logging information of Network State Machine (NSM). Optional keywords **status, events** or **timers** can be used with this command to get log information on these specific NSM events. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption nsm** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption nsm <status | events | timers>**

delete protocols ospf [instance-id <*instance-id***>] traceoption nsm <status | events | timers>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
nsm <status | events | timers>	Optional. Specifies to enable NSM logging for **status**, **events** or **timers** events.

Example

- Enable OSPF NSM logging for status related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption NSM status
admin@Xorplus# commit
```

set protocols ospf traceoption packet

Run the command **set protocols ospf traceoption packet** to enable OSPF packet logging. Optional keywords can be used for logging information on specific packet types. These types are **hello, dd** (database description packets), **ls-request** (link-state request), **ls-update** (link-state update), **ls-ack** (link-state acknowledgement) and **all**. Optionally you can choose packet event type **send** or **receive**. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run **delete protocols ospf traceoption packet** the command to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption packet {hello | dd | ls-request | ls-update | ls-ack | all } [send | recv | detail]**

delete protocols ospf [instance-id <*instance-id***>] traceoption packet {hello | dd | ls-request | ls-update | ls-ack | all } [send | recv | detail]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
packet {hello|dd|ls-request|ls-update|ls-ack|all}	Specifies to enable OSPF logging for **hello,** database description **(dd),** link state request **(ls-request),** link state update **(ls-update),** link state acknowledgement **(ls-ack)** or **all**.
send|recv|detail	Optional. Specifies the send or receive direction and details.

Example

- Enable detailed OSPF hello packet logging.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption packet hello detail
admin@Xorplus# commit
```

set protocols ospf traceoption zebra

Run the command **set protocols ospf traceoption zebra** to enable OSPF zebra module related logging. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption zebra** to remove this configuration from the database.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption zebra**

delete protocols ospf [instance-id <*instance-id***>] traceoption zebra**

Example

- Enable OSPF zebra module related logging for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption zebra
admin@Xorplus# commit
```

set protocols ospf graceful-restart enable

Run the command **set protocols ospf graceful-restart enable** to enable the OSPF Graceful Restart (GR) capability on the restarting device. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. By default, OSPF GR capability is disabled.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart enable** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) capability.
false	Disables OSPF Graceful Restart (GR) capability.

Usage Guidelines

To avoid traffic interruption and route oscillation caused by failover events, you can enable OSPF GR functionality on the restarting device by executing this command.

Example

- Enable OSPF Graceful Restart (GR) capability on the restarting device.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart enable true
admin@PICOS# commit
```

set protocols ospf capability opaque

Run the command **set protocols ospf capability opaque** to enable the capability to generate Opaque LSAs in the OSPF process, allowing the OSPF process to generate Opaque LSAs and receive them from neighboring devices. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf capability opaque** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] capability opaque**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] capability opaque**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

Opaque LSAs provide a generic mechanism for OSPF extensions, supporting the OSPF Graceful Restart (GR) feature through Type 9 LSAs. Therefore, before configuring OSPF GR, you must enable OSPF's Opaque LSA capability using this command.

Example

- Enable the capability to generate Opaque LSAs in the OSPF process.

```
admin@PICOS# set protocols ospf instance-id 1 capability opaque
admin@PICOS# commit
```

set protocols ospf graceful-restart grace-period

Run the command **set protocols ospf graceful-restart grace-period** to configure the maximum restart wait time. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart grace-period** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] grace-period <***grace-period***>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] grace-period**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
grace-period <*grace-period***>**	Specifies the maximum restart wait time, in seconds, advertised to neighbors. The value is an integer that ranges from 1 through 1800 seconds. The default value is 120 seconds.

Example

- Configure the maximum restart wait time.

```
admin@PICOS# set protocols ospf instance-id 1 grace-period 300
admin@PICOS# commit
```

set protocols ospf graceful-restart helper enable

Run the command **set protocols ospf graceful-restart helper enable** to enable the OSPF Graceful Restart (GR) Helper capability. By default, helper support is disabled for all neighbors. This config enables/disables helper support on this router for all neighbors. To enable/disable helper support for a specific neighbor, the router-id (A.B.C.D) has to be specified.

Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. By default, OSPF GR Helper capability is disabled.

- If helper is enabled for specific neighbors, the global helper configuration for other neighbors will not take effect.
- Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper enable** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) Helper capability.
false	Disables OSPF Graceful Restart (GR) Helper capability.
router-id <*ipv4*>	Optional. Specifies the router-id (A.B.C.D) of the neighbor device to enable/disable helper support for a specific neighbor.

Example

- Enable OSPF Graceful Restart (GR) Helper capability.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper enable true
admin@PICOS# commit
```

set protocols ospf graceful-restart helper planned-only

Run the command **set protocols ospf graceful-restart helper planned-only** to enable the OSPF Graceful Restart (GR) Helper to support only Planned Graceful Restart. By default, the device supports both Planned Graceful Restart and Unplanned Graceful Restart. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper planned-only** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper planned-only**

delete protocols ospf [instance-id <*instance-id***>] [vrf <***vrf-name***>] graceful-restart helper planned-only**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable the OSPF Graceful Restart (GR) Helper to support only Planned Graceful Restart.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper planned-only
admin@PICOS# commit
```

set protocols ospf graceful-restart helper strict-lsa-checking

Run the command **set protocols ospf graceful-restart helper strict-lsa-checking** to configure strict LSA checking on the Helper Router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Strict LSA checking is enabled by default.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper strict-lsa-checking** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper strict-lsa-checking enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper strict-lsa-checking enable <true | false>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables strict LSA checking.
false	Disables strict LSA checking.

Usage Guidelines

The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. You can enable strict LSA checking on an OSPF helper to have the router terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router. This feature takes effect only when the router is in helper mode.

Example

- Enable strict LSA checking on the Helper Router.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper strict-lsa-checking enable true
admin@PICOS# commit
```

set protocols ospf graceful-restart helper supported-grace-time

Run the command **set protocols ospf graceful-restart helper supported-grace-time** to configure the period for Graceful Restart on the Helper router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper supported-grace-time** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper supported-grace-time <***supported-grace-time***>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper supported-grace-time**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
supported-grace-time <*supported-grace-time***>**	Specifies the period for Graceful Restart on the Helper router. The value is an integer that ranges from 10 through 1800 seconds. There is no default value.

Example

- Configure the period for Graceful Restart on the Helper router.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper supported-grace-time 300
admin@PICOS# commit
```

run graceful-restart prepare ospf

The **run graceful-restart prepare ospf** command is a operational command that the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain, informing its neighbors about its restarting process and the estimated time for the restart to complete. These LSAs are Type 9 LSAs and are flooded throughout the OSPF domain.

The OSPF protocol should be restarted during the grace period, otherwise the graceful restart will fail.

To perform a graceful shutdown, this operational command needs to be issued before restarting the OSPF protocol.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

Command Syntax

run graceful-restart prepare ospf

Parameters

None.

Example

- Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain.

```
admin@Xorplus# run graceful-restart prepare ospf
```

run show ospf graceful-restart helper

Run the command **run show ospf graceful-restart helper** to display the Graceful Restart Helper details including helper config changes.

Command Syntax

run show ospf [**instance-id <***instance-id***>**][**vrf<***vrf-name***>**] **graceful-restart helper [detail]**

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display the Graceful Restart Helper details including helper config changes.

```
admin@PICOS# run show ospf graceful-restart helper
OSPF Router with ID (2.2.2.2)
 Graceful restart helper support enabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

set protocols ospf interface authentication-key

Run the command **set protocols ospf interface authentication-key** to set the authentication password that is used for simple-text authentication on the OSPF interface.
The command **delete protocols ospf interface authentication-key** deletes the OSPF interface authentication password that is used for simple-text authentication.

NOTE:

The command **set protocols ospf interface** <*interface-name*> **authentication address** <*ipv4*> is a mandatory configuration for setting the authentication address used for OSPF authentication.

Command Syntax

set protocols ospf interface <*interface-name*> **address** <*ipv4*> **authentication-key** <*PASSWORD*>

delete protocols ospf interface <*interface-name*> **address** <*ipv4*> **authentication-key**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Specifies an IPv4 address.
authentication-key <*PASSWORD*>	Specifies the password for simple-text authentication. The value is a string of 6 to 8 characters.

Example

- Configure OSPF authentication password on the interface address.

```
admin@XorPlus# set protocols ospf interface vlan200 address 10.10.114.1 authentication-key asjlfk
admin@Xorplus# commit
```

OSPFv3 Command Reference

- set protocols ospf6 area
- set protocols ospf6 area range
- set protocols ospf6 area stub
- set protocols ospf6 area stub no-summary
- set protocols ospf6 auto-cost reference-bandwidth
- set protocols ospf6 distance
- set protocols ospf6 distance-ospf6
- set protocols ospf6 interface area
- set protocols ospf6 interface cost
- set protocols ospf6 interface dead-interval
- set protocols ospf6 interface hello-interval
- set protocols ospf6 interface ifmtu
- set protocols ospf6 interface mtu-ignore
- set protocols ospf6 interface network
- set protocols ospf6 interface passive
- set protocols ospf6 interface priority
- set protocols ospf6 interface retransmit-interval
- set protocols ospf6 interface transmit-delay
- set protocols ospf6 log-adjacency-changes
- set protocols ospf6 redistribute
- set protocols ospf6 router-id
- set protocols ospf6 stub-router administrative
- set protocols ospf6 timers lsa min-arrival
- set protocols ospf6 timers throttle spf
- set protocols ospf6 traceoption
- set protocols ospf6 traceoption border-routers
- set protocols ospf6 traceoption lsa
- set protocols ospf6 traceoption message
- set protocols ospf6 traceoption neighbor
- set protocols ospf6 traceoption route
- set protocols ospf6 traceoption spf
- set protocols ospf6 traceoption zebra
- set protocols ospf6 graceful-restart enable
- set protocols ospf6 capability opaque
- set protocols ospf6 graceful-restart grace-period
- set protocols ospf6 graceful-restart helper enable
- set protocols ospf6 graceful-restart helper planned-only
- set protocols ospf6 graceful-restart helper lsa-checking-disable
- set protocols ospf6 graceful-restart helper supported-grace-time
- run graceful-restart prepare ospf6
- run show ospf6 graceful-restart helper

set protocols ospf6 area

Use the command **set protocols ospf6 area** to configure area for the OSPFv3 instance.

Run the command **delete protocols ospf6 area** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area{<***ipv4***> | <***area-id***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area{<***ipv4***> | <***area-id***>}**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area{<*ipv4***> | <***area-id***>}**	Specifies the area for OSPFv3, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures the OSPFv3 area ID to 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 area 0.0.0.0
```

set protocols ospf6 area range

Run the command **set protocols ospf6 area range** to configure a summary route for all the routes in that range. The range parameter is used on the ABRs for the purpose of managing the size of the routing table.

Run the command **delete protocols ospf6 area range** to remove this configuration from the switch.

Command Syntax

set protocol ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} range <***ipv6/prefixlen***>** [**advertise <true | false>** | **cost** <*cost*>]

delete protocol ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} range <***ipv6/prefixlen***>** [**advertise <true | false>** | **cost** <*cost*>]

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4*>|<*area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
range <*ipv6/prefixlen***>**	Specifies the range parameter, the value is in IPv6/prefix length format.
advertise <true | false>	Optional. Determines whether to advertise the summarized route or not. The value could be **true** or **false**. • **true**: Advertise the summarized route. • **false**: Do not advertise the summarized route. By default, the summarized route is advertised.
cost <*cost***>**	Optional. Specifies the cost of the summarized route. The value is an integer that ranges from 0 to 16777215.

Example

- This example creates a summary route for all the routes in the range 2001::/64.

```
admin@XorPlus# set protocols ospf6 area 0.0.0.0 range 2001::/64
```

set protocols ospf6 area stub

Run the command **set protocols ospf6 area stub** to configure a stub area for the OSPFv3 instance.

Run the command **delete protocols ospf6 area stub** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4*>|<*area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures area 1.1.1.1 as a stub area of the OSPFv3 instance in the default VRF.

```
admin@XorPlus# set protocols ospf6 area 1.1.1.1 stub
```

set protocols ospf6 area stub no-summary

Run the command **set protocols ospf6 area stub no-summary** to configure a stub area with no-summary option. The no-summary option disallows the injection of summary routes into an area and thus makes the area a *totally-stubby* area.

Run the command **delete protocols ospf6 area stub no-summary** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub no-summary**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub no-summary**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4*>|<*area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures area 1.1.1.1 as a totally-stubby area of the OSPFv3 instance in the default VRF.

```
admin@XorPlus# set protocols ospf6 area 1.1.1.1 stub no-summary
```

set protocols ospf6 auto-cost reference-bandwidth

Run the command **set protocols ospf6 auto-cost reference-bandwidth** to set the reference bandwidth for automatic route cost calculation. The reference bandwidth specified here is considered equivalent to OSPF cost of 1. The default bandwidth is 100Mbits/s, that is, a link with bandwidth of 100Mbits/s or higher is considered to have a cost of 1. Cost of links with lower bandwidth will be calculated with reference to this bandwidth value.

Note that this configuration must be consistent within the OSPF domain.

Run the command **delete protocols ospf6 auto-cost reference-bandwidth** to delete this configuration

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **auto-cost reference-bandwidth**<*ref-bandwidth*>

delete protocols ospf6 [**vrf** <*vrf-name*>] **auto-cost reference-bandwidth**<*ref-bandwidth*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
reference-bandwidth <*ref-bandwidth*>	Specifies the reference bandwidth. The value is an integer that ranges from 1 to 4294967.

Example

- Configure the OSPFv3 reference bandwidth to 500000.

```
admin@XorPlus# set protocols ospf6 auto-cost reference-bandwidth 500000
admin@Xorplus# commit
Commit Ok.
Save done
```

set protocols ospf6 distance

The command **set protocols ospf6 distance** configures the administrative distance for an entire group of OSPFv3 routes.

Run the command **delete protocols ospf6 distance** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **distance <***distance***>**

delete protocols ospf6 [**vrf** <*vrf-name*>] **distance** <*distance*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
distance <*distance***>**	Specifies the administrative distance, the value is an integer that ranges from 1 to 255

Example

- This example configures the administration distance of OSPF routes to 140.

```
admin@XorPlus# set protocols ospf6 distance 140
```

set protocols ospf6 distance-ospf6

Run the command **set protocols ospf6 distance-ospf6** to configure the administrative distance for intra-area, inter-area and external routes.

Run the command **delete protocols ospf6 distance-ospf6** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **distance-ospf6 {intra-area <***distance***> | inter-area <***distance***> | external <***distance***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **distance-ospf6 {intra-area <***distance***> | inter-area <***distance***> | external <***distance***>}**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
intra-area <*distance***>**	Specifies the administrative distance for intra-area routes. The values is an integer that ranges from 1 to 255.
inter-area <*distance***>**	Specifies the administrative distance for inter-area routes. The values is an integer that ranges from 1 to 255.
external <*distance***>**	Specifies the administrative distance for external routes. The values is an integer that ranges from 1 to 255.

Example

- This example configures the administrative distance of inter-area routes and intra-area routes to 200 and sets the administrative distance for external routes to 250.

```
admin@XorPlus# set protocols ospf6 distance ospf6 intra-area 200
admin@XorPlus# set protocols ospf6 distance-ospf6 inter-area 200
admin@XorPlus# set protocols ospf6 distance-ospf6 external 250
admin@XorPlus# commit
```

set protocols ospf6 interface area

Run the command **set protocols ospf6 interface area** to enable OSPFv3 on a specific interface and map that interface to an area.

Run the command **delete protocols ospf6 interface** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **area <***ipv4***>**

delete protocols ospf6 interface <*interface-name***> area <***ipv4***>**

Parameters

Parameter	Description
area <*ipv4***>**	Specifies the area for OSPFv3, the value is in IPv4 dotted decimal format.
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Usage Guidelines

You can add the L3 interface to a specified VRF to specify the VRF for the OSPFv3 instance. If L3 VLAN interface/loopback interface is not added to a specified VRF, then the command takes effect in the default VRF.

The following commands add the L3 VLAN interface to a specified VRF and specify the VRF for the OSPFv3 instance.

```
admin@XorPlus# set l3-interface vlan-interface vlan100 vrf "vrf1"
admin@XorPlus# set protocols ospf6 interface vlan100 area 0.0.0.0
```

Example

- This example enable OSPFv3 on L3 VLAN interface vlan100 and bind the interface to area 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 interface vlan100 area 0.0.0.0
```

set protocols ospf6 interface cost

Run the command **set protocols ospf6 interface cost** to set the OSPF link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation. Changing the interface cost causes the OSPF to run the SPF and reissue LSAs.

Run the command **delete protocols ospf6 interface cost** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **cost** <*1-65535*>

delete protocols ospf6 interface <*interface-name*> **cost**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
cost <*1-65535*>	Specifies the link cost, the value is an integer in the range of 1 to 65535.

Example

- Set the OSPFv3 interface vlan200 cost to 5.

```
admin@XorPlus# set protocols ospf6 interface vlan200 cost 5
admin@Xorplus# commit
```

set protocols ospf6 interface dead-interval

Run the command **set protocols ospf6 interface dead-interval** to configure the OSPF neighbor router dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf6 interface dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **dead-interval** <*1-65535*>

delete protocols ospf interface <*interface-name*> **dead-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dead-interval <*1-65535*>	Specifies the OSPFv3 neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPFv3 neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf6 interface hello-interval

Run the command **set protocols ospf6 interface hello-interval** to set the OSPF hello interval on the specified interface. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf interface hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **hello-interval** <*1-65535*>

delete protocols ospf interface <*interface-name*> **hello-interval** <*1-65535*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
hello-interval <*1-65535*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on interface vlan200.

```
admin@XorPlus# set protocols ospf6 interface vlan200 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf6 interface ifmtu

Run the command **set protocols ospf6 interface ifmtu** to configure the OSPFv3 interface MTU.

Run the command **delete protocols ospf6 interface ifmtu** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> ifmtu <***1-65535***>**

delete protocols ospf6 interface <*interface-name***> ifmtu <***1-65535***>**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
ifmtu <*1-65535***>**	Specifies the OSPFv3 interface MTU, the value is an integer that ranges from 1 to 65535.

Example

- Set the OSPFv3 interface MTU to 1400.

```
admin@XorPlus# set protocols ospf6 interface vlan200 ifmtu 1400
admin@Xorplus# commit
```

set protocols ospf6 interface mtu-ignore

Run the command **set protocols ospf6 interface mtu-ignore** to disable ignore MTU mismatch detection on this interface.

Run the command **delete protocols ospf6 interface mtu-ignore** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **mtu-ignore**

protocols ospf6 interface <*interface-name*> **mtu-ignore**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- This example configures the MTU mismatch detection on the interface *vlan10.*

```
admin@XorPlus# set protocols ospf6 interface vlan10 mtu-ignore
admin@XorPlus# commit
```

set protocols ospf6 interface network

Run the command **set protocols ospf6 interface network** to enable OSPF on an interface and specify a network type. Enabling OSPF on an interface allows the interface to send and receive LSAs. Two different network types can be specified here namely, **broadcast** and **point-to-point**.

To delete this configuration, run the command **delete protocols ospf interface network**

Command Syntax

set protocols ospf interface <*interface-name*> **network <broadcast|point-to-point>**

delete protocols ospf interface <*interface-name*> **network <broadcast|point-to-point>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
broadcast	Specifies the OSPF broadcast multi-access network.
point-to-point	Specifies the OSPF point-to-point network.

Example

- Enable OSPFv3 on interface vlan200 and specify network type as point-to-point.

```
admin@XorPlus# set protocols ospf interface vlan200 network point-to-point
admin@Xorplus# commit
```

set protocols ospf6 interface passive

Run the command **set protocols ospf6 interface passive** to identify a specific interface as OSPFv3 passive interface. Passive interfaces are part of OSPFv3 database but they do not send or receive OSPF LSAs. OSPFv3 does not try to form adjacency relationship with peers on these interfaces.

Run the command **delete protocols ospf6 interface passive** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> passive**

delete protocols ospf6 interface <*interface-name***> passive**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- Set the interface vlan200 as OSPFv3 passive interface.

```
admin@XorPlus# set protocols ospf6 interface vlan200 passive
admin@Xorplus# commit
```

set protocols ospf6 interface priority

Run the command **set protocols ospf6 interface priority** to set the interface's router priority. The default value is 1.

Run the command **delete protocols ospf6 interface priority** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> priority <***priority***>**

delete protocols ospf6 interface <*interface-name*> **priority <***priority***>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
priority <*priority***>**	Specifies the interface's router priority, the value is an integer that ranges from 0 to 255. The default value is 1.

Example

- Set the interface vlan200 router priority to 2.

```
admin@XorPlus# set protocols ospf6 interface vlan200 priority 2
admin@Xorplus# commit
```

set protocols ospf6 interface retransmit-interval

Run the command **set protocols ospf6 interface retransmit-interval** to configure the LSA retransmit interval for adjacencies belonging to the OSPFv3 interface for lost LSAs.

Run the command **delete protocols ospf6 interface retransmit-interval** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **retransmit-interval <***seconds***>**

delete protocols ospf6 interface <*interface-name*> **retransmit-interval <***seconds***>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
retransmit-interval <*seconds***>**	Specifies the LSA retransmit interval for the OSPFv3 interface in seconds. The value is an integer that ranges from 1 to 65535.

Example

- Set the retransmit interval for lost LSAs for the OSPFv3 interface to 10 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 retransmit-interval 10
admin@Xorplus# commit
```

set protocols ospf6 interface transmit-delay

Run the command **set protocols ospf6 interface transmit-delay** to set the estimated time needed to send an OSPFv3 LSA update packet.

Run the command **delete protocols ospf6 interface transmit-delay** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 interface *<interface-name>* **transmit-delay <***seconds***>**

delete protocols ospf6 interface *<interface-name>* **transmit-delay <***seconds***>**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
transmit-delay <*seconds***>**	Specifies the transmit delay in seconds, the value is an integer that ranges from 1 to 3600.

Example

- Set the OSPFv3 interface transmit delay to 20 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 transmit-delay 20
admin@Xorplus# commit
```

set protocols ospf6 log-adjacency-changes

Run the command **set protocols ospf6 log-adjacency-changes** to enable logging OSPFv3 adjacency changes. The optional parameter **detail** can be used to log all adjacency status changes. Without the **detail** keyword, only the adjacency changes to full or regression are logged.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **log-adjacency-changes [detail]**

delete protocols ospf6 [**vrf** <*vrf-name*>] **log-adjacency-changes [detail]**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.

Example

- This example enables all OSPFv3 adjacency changes logging.

```
admin@XorPlus# set protocols ospf6 log-adjacency-changes detail
admin@XorPlus# commit
```

set protocols ospf6 redistribute

Run the command **set protocols ospf6 redistribute** to redistribute routes from other sources and protocols through OSPFv3. Users can add the **route-map** parameter to include a route map to filter routes before redistribution.

To delete this configuration, run the command **delete protocols ospf6 redistribute.**

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **redistribute {bgp|connected|kernel|isis|ripng|static|table} [route-map<***route-map***>]**

delete protocols ospf6 [**vrf** <*vrf-name*>] **redistribute {bgp|connected|kernel|isis|ripng|static|table} [route-map<***route-map***>]**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
isis	Specify IS-IS routes for redistribution into OSPF.
ripng	Specify RIPng routes for redistribution into OSPF.
static	Specifies the static routes for redistribution.
table	Redistribute routes from table.
route-map<*route-map***>**	Optional. Specifies a route map for filtering routes before redistribution.

Example

- Configure OSPFv3 to redistribute BGP routes into OSPFv3 and apply route-map *map1* for route filtering.

```
admin@XorPlus# set protocols ospf6 redistribute bgp route-map map1
admin@Xorplus# commit
```

set protocols ospf6 router-id

Run the command **set protocols ospf6 router-id** to configure OSPFv3 router ID. The router ID should be unique within the OSPF domain and is in the IPv4 dotted decimal format.

Run the command **delete protocols ospf route-id** to delete this configuration.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **router-id** <ipv4>

delete protocols ospf6 [**vrf** <*vrf-name*>] **router-id** <ipv4>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
router-id <ipv4>	Specify OSPFv3 router ID. The value is in IPv4 dotted decimal format.

Example

- Configure OSPFv3 router ID.

```
admin@XorPlus# set protocols ospf6 router-id 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf6 stub-router administrative

Run the command **set protocols ospf6 stub-router administrative** to make a router a stub router for indefinite period of time.

Run the command **delete protocols ospf6 stub-router administrative** to delete this configuration.

Command Syntax

set protocol ospf6 [**vrf** <*vrf-name*>] **stub-router administrative**

delete protocol ospf6 [**vrf** <*vrf-name*>] **stub-router administrative**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.

Example

- This example configures OSPF stub router for an indefinite period of time.

```
admin@XorPlus# set protocols ospf6 stub-router administrative
admin@Xorplus# commit
```

set protocols ospf6 timers lsa min-arrival

Run the command **set protocols ospf6 timers lsa min-arrival** to set the minimum delay in receiving a new version of an LSA. The value of this parameter is in milliseconds and ranges from 0 to 600000.

Run the command **delete protocols ospf6 timers lsa min-arrival** to remove this configuration and go back to default delay of 1000 milliseconds.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **timers lsa min-arrival** <*milliseconds*>

delete protocols ospf6 [**vrf** <*vrf-name*>] **timers lsa min-arrival** <*milliseconds*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
min-arrival <*milliseconds*>	Specify the minimum delay in receiving a new LSA in milliseconds. The value is an integer that ranges from 0 to 600000.

Example

- Configure OSPFv3 minimum delay to receive LSA to 2000 milliseconds.

```
admin@XorPlus# set protocols ospf6 timers lsa min-arrival 2000
admin@Xorplus# commit
```

set protocols ospf6 timers throttle spf

Run the command **set protocols ospf6 timers throttle spf** to set the initial *delay,* the *initial hold-time* and the *maximum hold-time* between when the SPF is calculated and the event which triggered the calculation. These timers prevents the system from overburdening the CPU with frequent SPF calculations.

Run the command **delete protocols ospf timers throttle spf** to delete this configuration.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **timers throttle spf {delay<***delay***> | initial-holdtime<***nitial-hold-time***> | maximum-holdtime<***max-hold-time***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **timers throttle spf {delay**<*delay*> **| initial-holdtime**<*delay*> **| maximum-holdtime**<*max-hold-time*>**}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
delay<*delay***>**	Specifies the *initial delay*, the value ranges from 0 to 600000 milliseconds.
initial-holdtime<*nitial-hold-time***>**	Specifies the *initial hold time*, the value ranges from 0 to 600000 milliseconds.
maximum-holdtime<*max-hold-time*>	Specifies the *maximum hold time*, the value ranges from 0 to 600000 milliseconds.

Usage Guidelines

These three parameters are important fine tuning tools for OSPFv3. These timers are introduced to delay starting SFP calculations when a SPF-triggering event occurs. Frequent SPF calculations may incur heavy burden on the device resources such as CPU especially in large OSPFv3 networks. The *delay* parameter specifies the delay in SPF calculation. This delay also applies to events occurring outside the *hold-time* of the previous SPF calculation. Two consecutive SPF calculations are always delayed by at least hold-time delay in milliseconds. The hold-time is initially set to the *initial hold-time* but its value is flexible and may be changed. If an event occurs within the hold-time of the previous SPF calculation, it results in increasing the hold-time by *initial hold-time.* If the flexible hold-time expires and no SPF triggering event occurs, the hold-time is reset to *initial hold-time.*

The example below sets the initial *delay* to 20ms, *initial hold-time* to 50ms and *maximum hold-time* to 5 seconds. This means that there will be a delay of 20ms between an SPF-triggering event and the commencement of the actual SPF calculation. The delay between two consecutive SPF calculations will be between 50ms and 5 seconds. If an SPF-triggering event occurs between the hold-time of the previous SPF calculation, the hold-time is increased by 50ms.

Example

- Configure OSPFv3 SPF times of initial delay, initial hold-time and maximum hold-time to 20ms, 50ms and 5000ms respectively.

```
admin@XorPlus# set protocols ospf6 timers throttle spf delay 20
admin@XorPlus# set protocols ospf6 timers throttle spf initial-holdtime 50
admin@XorPlus# set protocols ospf6 timers throttle spf maximum-holdtime 5000
admin@Xorplus# commit
```

set protocols ospf6 traceoption

Run the command **set protocols ospf6 traceoption** to enable debugging for the OSPFv3 instance. Debugging information can be enabled for different features of OSPFv3 such as **abr** (Area Border Router), **asbr** (Autonomous System Border Router), **flooding** or **interface**.

To remove the configuration, run the command **delete protocols ospf6 traceoption.**

Command Syntax

set protocols ospf6 traceoption <abr | asbr | flooding | interface>

delete protocols ospf6 traceoption <abr | asbr | flooding | interface>

Parameters

Parameter	Description
abr	Choose this parameter to enable debugging related to OSPFv3 ABR events.
asbr	Choose this parameter to enable debugging related to OSPFv3 ASBR events.
flooding	Choose this parameter to enable debugging related to OSPFv3 flooding events.
interface	Choose this parameter to enable debugging related to OSPFv3 interface events.

Example

- This example enables OSPFv3 debugging for flooding events.

```
admin@XorPlus# set protocols ospf6 traceoption flooding
```

set protocols ospf6 traceoption border-routers

Run the command **set protocols ospf6 traceoption border-routers** to enable or disable border routers relation debug information. Optional parameters **area-id** or **router-id** can be used to specify the area ID or router ID for which to enable/disable debug information.

Run the command **delete protocols ospf6 traceoption border-routers** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption border-routers [area-id <*ipv4***> | router-id <***ipv4***>]**

delete protocol ospf6 traceoption border-routers [area-id <*ipv4***> | router-id <***ipv4***>]**

Parameters

Parameter	Description
area <*ipv4***>**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
router-id <*ipv4***>**	Specifies the router ID, the value is in IPv4 dotted decimal format.

Example

- This example enables border routers debug information for area 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 border-routers area-id 0.0.0.0
```

set protocols ospf6 traceoption lsa

Run the command **set protocols ospf6 traceoption lsa** to enable debug information related to Link State Advertisement. The user can choose different components of OSPFv3 while enabling or disabling LSA related debug info such as **router**, **network** etc.

To remove this configuration, run the command **delete protocols traceoption lsa**

Command Syntax

set protocols ospf6 traceoption lsa <router | network | inter-prefix | inter-router | as-external | link | intra-prefix | unknown> [originate | examine | flooding]

delete protocol ospf6 traceoption lsa <router | network | inter-prefix | inter-router | as-external | link | intra-prefix | unknown> [originate | examine | flooding]

Example

- This example enables LSA debugging for routers.

```
admin@XorPlus# set protocols ospf6 lsa router
```

set protocols ospf6 traceoption message

Run the command **set protocols ospf6 traceoption message** to enable or disable OSPFv3 messages related debugging. The user can choose from a range of different packet types while enablling/disabling debug information such as unknow packets, hello packets etc. Optionally, the user can choose between packets sent or received for debugging.

Run the command **delete protocols ospf6 traceoption message** to delete this configuration.

Command Syntax

set protocols ospf6 traceoption message <unknown | hello | dbdesc | lsreq | lsupdate | lsack | all> [send|recv]

delete protocols ospf6 traceoption message <unknown | hello | dbdesc | lsreq | lsupdate | lsack | all> [send|recv]

Parameters

Parameter	Description
unknown	Specifies unknow packets.
hello	Specifies OSPFv3 hello packets.
dbdesc	Specifies OSPFv3 database description packets.
lsreq	Specifies Link State Request packets.
lsupdate	Specifies Link State Update packets.
lsack	Specifies Link State ACK packets.
all	Specifies debugging of all packets.
send	Optional. Specifies packets sent.
recv	Optional. Specifies packets received.

Example

- This example enables the OSPFv3 received link state update packet debugging.

```
admin@XorPlus# set protocols ospf6 traceoption lsupdate recv
```

set protocols ospf6 traceoption neighbor

Run the command **set protocols ospf6 traceoption neighbor** to enable OSPFv3 neighbor related debugging. The user can choose between **state** or **event** related debugging information or can choose **all** to enable all debugging related to neighbor state change.

Run the command **delete protocols ospf6 traceoption neighbor** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption neighbor <state | event | all>

delete protocols ospf6 traceoption neighbor <state | event | all>

Example

- This example enables OSPFv3 neighbor state related debugging.

```
admin@XorPlus# set protocols ospf6 neighbor state
```

set protocols ospf6 traceoption route

Run the command **set protocols ospf6 traceoption route** to enable route related debugging. The user can choose between different types of route debugging options such as **table, inter-area** etc to get debugging related to these specific events. Its important to note that inter-area routes are those routes which are created from Router LSAs and Network LSAs. Also to get information about memory usage of the routes, the user can choose the option **memory.** To get route debugging for the routing table then the user can choose the option **table.**

Run the command **delete protocols ospf6 traceoption route** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption route {table|intra-area|inter-area|memory}

delete protocol ospf6 traceoption route {table|intra-area|inter-area|memory}

Example

- This example configures OSPFv3 debugging for inter-area routes.

```
admin@XorPlus# set protocols ospf6 traceoption inter-area
```

set protocols ospf6 traceoption spf

Run the command **set protocols ospf6 traceoption spf** to enable the OSPFv3 SPF related debugging. The user can append **database** or **process** or **time** to enable specific SPF debugging. The **database** option enables logging of the number of LSAs at SPF calculation time. The **process** keyword will enable detailed debugging of the entire SPF process. The **time** option enables debugging of time taken by SPF calculation.

Run the command **delete protocols ospf6 traceoption spf** to delete this configuration.

Command Syntax

set protocols ospf6 traceoption spf <database | process | time>

delete protocols ospf6 traceoption spf <database | process | time>

Example

- This example configures the OSPFv3 SPF database related debugging.

```
admin@XorPlus# set protocols ospf6 traceoption spf database
```

set protocols ospf6 traceoption zebra

Run the command **set protocols ospf6 traceoption zebra** to configure OSPFv3 zebra module related debugging. Use the arguments **send, recv** or **all** to specify debugging for either packets sent, received or both.

Run the command **delete protocols ospf6 traceoption zebra** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption zebra <send | recv | all>

delete protocols ospf6 traceoption zebra <send | recv | all>

Example

- This example configures the OSPFv3 zebra module packet debugging for packets received.

```
admin@XorPlus# set protocols ospf6 traceoption zebra received
```

set protocols ospf6 graceful-restart enable

Run the command **set protocols ospf6 graceful-restart enable** to enable the OSPFv3 Graceful Restart (GR) capability on the restarting device. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. By default, OSPF GR capability is disabled.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart enable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart enable <true | false>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) capability.
false	Disables OSPF Graceful Restart (GR) capability.

Usage Guidelines

To avoid traffic interruption and route oscillation caused by failover events, you can enable OSPFv3 GR functionality on the restarting device by executing this command.

Example

- Enable OSPFv3 Graceful Restart (GR) capability on the restarting device.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart enable true
admin@PICOS# commit
```

set protocols ospf6 capability opaque

Run the command **set protocols ospf6 capability opaque** to enable the capability to generate Opaque LSAs in the OSPFv3 process, allowing the OSPFv3 process to generate Opaque LSAs and receive them from neighboring devices. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 capability opaque** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] capability opaque**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] capability opaque**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

Opaque LSAs provide a generic mechanism for OSPFv3 extensions, supporting the OSPFv3 Graceful Restart (GR) feature through Type 9 LSAs. Therefore, before configuring OSPFv3 GR, you must enable OSPF's Opaque LSA capability using this command.

Example

- Enable the capability to generate Opaque LSAs in the OSPFv3 process.

```
admin@PICOS# set protocols ospf6 instance-id 1 capability opaque
admin@PICOS# commit
```

set protocols ospf6 graceful-restart grace-period

Run the command **set protocols ospf6 graceful-restart grace-period** to configure the maximum restart wait time. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart grace-period** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] grace-period <***grace-period***>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] grace-period**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
grace-period <*grace-period***>**	Specifies the maximum restart wait time, in seconds, advertised to neighbors. The value is an integer that ranges from 1 through 1800 seconds. The default value is 120 seconds.

Example

- Configure the maximum restart wait time.

```
admin@PICOS# set protocols ospf6 instance-id 1 grace-period 300
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper enable

Run the command **set protocols ospf6 graceful-restart helper enable** to enable the OSPFv3 Graceful Restart (GR) Helper capability. By default, helper support is disabled for all neighbors. This config enables/disables helper support on this router for all neighbors. To enable/disable helper support for a specific neighbor, the router-id (A.B.C.D) has to be specified.

Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF. By default, OSPF GR Helper capability is disabled.

- If helper is enabled for specific neighbors, the global helper configuration for other neighbors will not take effect.
- Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper enable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) Helper capability.
false	Disables OSPF Graceful Restart (GR) Helper capability.
router-id <*ipv4*>	Optional. Specifies the router-id (A.B.C.D) of the neighbor device to enable/disable helper support for a specific neighbor.

Example

- Enable OSPFv3 Graceful Restart (GR) Helper capability.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper enable true
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper planned-only

Run the command **set protocols ospf6 graceful-restart helper planned-only** to enable the OSPFv3 Graceful Restart (GR) Helper to support only Planned Graceful Restart. By default, the device supports both Planned Graceful Restart and Unplanned Graceful Restart. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper planned-only** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper planned-only**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper planned-only**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable the OSPFv3 Graceful Restart (GR) Helper to support only Planned Graceful Restart.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper planned-only
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper lsa-checking-disable

Run the command **set protocols ospf6 graceful-restart helper lsa-checking-disable** to configure strict LSA checking on the Helper Router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. OSPFv3 strict LSA checking is disabled by default.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper lsa-checking-disable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper strict-lsa-checking**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper strict-lsa-checking**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. You can enable strict LSA checking on an OSPF helper to have the router terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router. This feature takes effect only when the router is in helper mode.

Example

- Enable strict LSA checking on the Helper Router.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper lsa-checking-disable
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper supported-grace-time

Run the command **set protocols ospf6 graceful-restart helper supported-grace-time** to configure the period for Graceful Restart on the Helper router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper supported-grace-time** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper supported-grace-time <***supported-grace-time***>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper supported-grace-time**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
supported-grace-time <*supported-grace-time***>**	Specifies the period for Graceful Restart on the Helper router. The value is an integer that ranges from 10 through 1800 seconds. There is no default value.

Example

- Configure the period for Graceful Restart on the Helper router.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper supported-grace-time 300
admin@PICOS# commit
```

run graceful-restart prepare ospf6

The **run graceful-restart prepare ospf6** command is a operational command that the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain, informing its neighbors about its restarting process and the estimated time for the restart to complete. These LSAs are Type 9 LSAs and are flooded throughout the OSPF domain.

The OSPF protocol should be restarted during the grace period, otherwise the graceful restart will fail.

To perform a graceful shutdown, this operational command needs to be issued before restarting the OSPF protocol.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

Command Syntax

run graceful-restart prepare ospf6

Parameters

None.

Example

- Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain.

```
admin@Xorplus# run graceful-restart prepare ospf6
OSPFv3 Routing Process (0) with Router-ID 2.2.2.2
 Graceful restart helper support disabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

run show ospf6 graceful-restart helper

Run the command **run show ospf6 graceful-restart helper** to display the Graceful Restart Helper details including helper config changes.

Command Syntax

run show ospf6 [**instance-id <***instance-id***>**][**vrf<***vrf-name***>**] **graceful-restart helper [detail]**

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPFv3 instance ID. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display the Graceful Restart Helper details including helper config changes.

```
admin@PICOS# run show ospf6 graceful-restart helper
OSPFv3 Routing Process (0) with Router-ID 12.12.12.20
 Graceful restart helper support disabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

Static Route Configuration Commands

- set protocols static interface-route interface
- set protocols static mroute
- set protocols static route

set protocols static interface-route interface

The **set protocols static interface-route interface** command configures a unicast static route by specifying the outgoing interface.

The **delete protocols static interface-route interface** command removes the static route.

Command Syntax

set protocols static [vrf <*vrf-name*>**] interface-route** <*ip/prefixlen*> **interface** <*interface-name*> [**distance** <*distance*> | **tag** <*tag*>]

delete protocols static [vrf <*vrf-name*>**] interface-route** <*ip/prefixlen*> **interface** <*interface-name*> [**distance** <*distance*> | **tag** <*tag*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. If not specified, it will create a static route in the default VRF.
interface-route <*ip/prefixlen*>	Specifies a destination IPv4 or IPv6 address. Where *prefixlen* specifies the number of bits in the address mask in int format (x), where x is a decimal number from 1 to 32 for IPv4 and 1 to 128 for IPv6.
interface <*interface-name*>	Specifies the L3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.
tag <*tag*>	Optional. Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.

Example

• This example creates a static route.

```
admin@XorPlus# set protocols static interface-route 10.10.10.10/32 interface vlan100
admin@XorPlus# commit
```

set protocols static mroute

The **set protocols static mroute** command adds a static route entry to the Multicast RIB.

The **delete protocols static mroute** command removes the static route.

Command Syntax

set protocols static mroute <*ipv4/prefixlen*> {**next-hop**<*nexthop-address*> **| next-hop-interface** <*interface-name*>} [**distance** <*distance*>]

delete protocols static mroute <*ipv4/prefixlen*> **{next-hop<*nexthop-address*> | next-hop-interface <*interface-name*>} [distance**<*distance*>**]**

Parameter

Parameter	Description
mroute <*ipv4/prefixlen*>	Specifies the IPv4 address of a multicast source. The value is in dotted decimal notation. The value *prefixlen* is a decimal integer that ranges from 1 to 32.
next-hop<*nexthop-address*>	Specifies the next-hop address. The value is in dotted decimal notation.
next-hop-interface <*interface-name*>	Specifies the L3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.

Example

• This example creates a static route.

```
admin@XorPlus# set protocols static mroute 10.10.10.0/24 next-hop-interface vlan100
admin@XorPlus# commit
```

set protocols static route

The **set protocols static route** command configures a unicast static route by specifying the next hop.

The **delete protocols static route** command removes the static route.

Note:

- If you are configuring a default route in the default VRF, you need to enable management VRF (After enabled by using command set system management-vrf enable true, eth0 will automatically be moved to management VRF from default VRF) to ensure the normal access to eth0 management port.
- When configuring IPv6 static route on FS S5810 Series and S5860 Series switch, the value of "*prefixlen*" should be less than or equal to 64.

Command Syntax

set protocols static [vrf<*vrf-name*>**] route** <*ip/prefixlen*> {**next-hop** <*nexthop-address*> | **blackhole | null0 | reject}** [**distance** <*distance*> | **tag** <*tag*>]

delete protocols static [vrf<*vrf-name*>**] route** <*ipv4/prefixlen*> {**next-hop** <*nexthop-address*> | **blackhole | null0 | reject}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. If not specified, it will create a static route in the default VRF.
route <*ip/prefixlen*>	Specifies a destination IPv4 or IPv6 address. Where *prefixlen* specifies the number of bits in the address mask in int format (x), where x is a decimal number from 1 to 32 for IPv4 and 1 to 128 for IPv6.
next-hop <*nexthop-address*>	Specifies the next-hop address.
blackhole	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
null0	Specifies the NULL0 interface as an outgoing interface. All the IP packets destined for the destination address are discarded without notifying the source host.
reject	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.
tag <*tag*>	Optional. Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.

Example
• This example creates a static black hole route.

```
admin@XorPlus# set protocols static route 10.10.10.10/32 blackhole
admin@XorPlus# commit
```

Route Map Commands

- run show routing route-map
- set routing as-path-list
- set routing large-community-list expanded
- set routing large-community-list standard
- set routing prefix-list
- set routing prefix-list description
- set routing community-list expanded
- set routing community-list standard
- set routing extcommunity-list expanded
- set routing extcommunity-list standard
- set routing route-map set-action large-community
- set routing route-map call
- set routing route-map description
- set routing route-map match as-path
- set routing route-map match community
- set routing route-map match community-with-exact-match
- set routing route-map match evpn default-route
- set routing route-map match evpn route-type
- set routing route-map match evpn vni
- set routing route-map match extcommunity
- set routing route-map matching-policy
- set routing route-map match interface
- set routing route-map match ipv4-addr address
- set routing route-map match ipv4-addr next-hop
- set routing route-map match ipv4-addr route-source
- set routing route-map match ipv6-addr
- set routing route-map match large-community
- set routing route-map match local-preference
- set routing route-map match metric
- set routing route-map match origin
- set routing route-map match peer
- set routing route-map match source-protocol
- set routing route-map match source-vrf
- set routing route-map match tag
- set routing route-map on-match
- set routing route-map set-action aggregator
- set routing route-map set-action as-path exclude
- set routing route-map set-action as-path prepend
- set routing route-map set-action atomic-aggregate
- set routing route-map set-action comm-list-delete
- set routing route-map set-action community
- set routing route-map set-action community-additive
- set routing route-map set-action extcommunity
- set routing route-map set-action extcommunity bandwidth
- set routing route-map set-action extcommunity bandwidth-non-transitive
- set routing route-map set-action ip-next-hop
- set routing route-map set-action ipv4-vpn-next-hop
- set routing route-map set-action ipv6-next-hop
- set routing route-map set-action label-index
- set routing route-map set-action large-comm-list-delete
- set routing route-map set-action local-preference
- set routing route-map set-action metric
- set routing route-map set-action metric-type
- set routing route-map set-action origin
- set routing route-map set-action originator-id
- set routing route-map set-action src
- set routing route-map set-action tag
- set routing route-map set-action weight

run show routing route-map

The **run show routing route-map** command to displays the configured route map information.

Command Syntax

run show routing route-map

Parameter

None.

Example

- View the configured route map information.

```
admin@Xorplus# run show routing route-map
ZEBRA:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
OSPF:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
    community COMMUNITY1
  Set clauses:
    community 11:101
  Call clause:
  Action:
    Exit routemap
```

set routing as-path-list

The **set routing as-path-list** command configures an AS Path list to match a specific AS path. AS Path lists are named lists of regular expression rules. They are used to match AS Path attributes in the routes for inclusion in or exclusion from route policies.

The **delete routing as-path-list** command removes the AS Path list configuration.

Command Syntax

set routing as-path-list <*as-path-list-name*> **{deny|permit} regex** <*txt*>

delete routing as-path-list <*as-path-list-name*> [**{deny|permit} regex** <*txt*>]

Parameter

Parameter	Description
as-path-list <*as-path-list-name*>	Specifies the name of the AS Path list.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
regex <*txt*>	Specifies the AS_Path regular expression (BGP Regular Expressions). The value is a string of 1 to 255 characters, space is not supported. **NOTE**: AS_Path regular expression doesn't support the specifial character ".", which results in unsupported filtering of AS numbers in asdot format.

Example

- Configure an AS Path list, permit routes that contain 20 in the AS_Path to pass through.

```
admin@Xorplus# set routing as-path-list Aslist permit regex _20_
admin@Xorplus# commit
```

set routing large-community-list expanded

The **set routing large-community-list expanded** command defines a new expanded large community list.

The **delete routing large-community-list expanded** command removes the expanded large community list configuration.

Command Syntax

set routing large-community-list {expanded <*large-community-list-name*>| **seq-expanded** <*integer*>} **{deny|permit} regex** <*line*>

delete routing large-community-list {expanded <*large-community-list-name*>**| seq-expanded** <*integer*>**} {deny|permit} regex** <*line*>

Parameter

Parameter	Description
expanded <*large-community-list-name*>	Specifies the name of the large community list that matches a route.
seq-expanded <*integer*>	Specifies an expanded large community list number from 100 to 500.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<*line*>	Specifies a string matching expression, it will be compared to the entire Large Communities attribute as a string, with each large-community in order from lowest to highest. line can also be a regular expression (BGP Regular Expressions) which matches this Large Community attribute.

Example

- Define a new expanded large community list.

```
admin@Xorplus# set routing large-community-list expanded Largecom1 permit regex _20
admin@Xorplus# commit
```

set routing large-community-list standard

The **set routing large-community-list standard** command defines a new standard large community list.

The **delete routing large-community-list standard** command removes the standard large community list configuration.

Command Syntax

set routing large-community-list {standard <*large-community-list-name***>| seq-standard**<*integer*>} **{deny|permit}** [**large-community** <*large-community-number*>]

delete routing large-community-list {standard <*large-community-list-name*>**| seq-standard**<*integer*>**} {deny|permit} [large-community** <*large-community-number*>**]**

Parameter

Parameter	Description
standard <*large-community-list-name***>**	Specifies the name of the large community list that matches a route.
seq-standard<*integer*>	Specifies an standard large community list number from 1 to 99.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
large-community <*large-community-number*>	Specifies the large community value. The value should be in a aa:bb:cc format. A maximum of 99 large community value can be configured.

Usage Guidelines

This command defines a new standard large-community-list. large-community is the Large Community value. We can add multiple large communities under same name. In that case the match will happen in the user defined order. Once the large-community-list matches the Large Communities attribute in BGP updates it will return permit or deny based upon the large-community-list definition. When there is no matched entry, a deny will be returned. When large-community is empty it matches any routes.

Example

- Define a new standard large community list.

```
admin@Xorplus# set routing large-community-list standard LargeCom deny large-community 6215:22:33
admin@Xorplus# commit
```

set routing prefix-list

The **set routing prefix-list** command creates an IPv4/IPv6 prefix list or an entry in an IPv4/IPv6 prefix list.

The **delete routing prefix-list** command deletes an IPv4/IPv6 prefix list or an entry from an IPv4/IPv6 prefix list.

Command Syntax

set routing prefix-list {ipv4-family <*ipv4-prefix-name*> | **ipv6-family** <*ipv6-prefix-name*>} [**seq** <*sequence-number*>] {**deny|permit} {prefix** <*ipaddress/prefixlen*> **[ge <***greater-equal-value***>] [le <***less-equal-value***>]** | **prefix-any**}

delete routing prefix-list {**ipv4-family** <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>} [**seq** <*sequence-number*>]**deny|permit} {prefix** <*ipaddress/prefixlen*> **[ge** <*greater-equal-value*>**] [le** <*less-equal-value*>**] | prefix-any}**

Parameter

Parameter	Description
<*ip4-prefix-name*>	Specifies the name of an IPv4 prefix list.
<*ip6-prefix-name*>	Specifies the name of an IPv6 prefix list.
seq <*sequence-number*>	Optional. Specifies the sequence number of an entry in the IP prefix list. The value is an integer that ranges from 1 to 4294967295. **NOTE:** When configuring IP prefix list, it is strongly recommended to configure sequence number for each IP prefix list node. Otherwise, the precedence of this IP prefix list will be uncertain, and thus the desired IP filtering effect will not be achieved.
{**deny|permit}**	Specifies whether the route is available for further processing when there is a match. The value could be **deny** or **permit**. • **deny**: In deny mode, if the IP address to be filtered is within the defined prefix range, the IP address fails to match the routing policy and cannot match the next entry. • **permit**: In permit mode, if the IP address to be filtered is within the defined prefix range, the IP address matches the routing policy and does not continue to match the next entry.
{prefix <*ipaddress/prefixlen*> | **prefix-any}**	Specifies an IP address/prefix length or all addresses. The value of prefix length is an integer that ranges from 1 to 32 for IPv4 addresses, and 1 to 128 for IPv6 addresses. When **prefix-any** is specified, it creates a prefix-list that matches all addresses.
ge <*greater-equal-value***>**	Optional. Specifies the lower threshold of the mask length. It can be used when an IP address/prefix length is specified. If **ge** *greater-equal-value* and **le** *less-equal-value* are not specified, the value of prefix length is the mask length. For IPv4: • *greater-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. • If only **ge** is configured, the mask ranges from *greater-equal-value* to 32. For IPv6: • *greater-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128. • If only **ge** is configured, the mask ranges from *greater-equal-value* to 128.
le <*less-equal-value***>**	Optional. Specifies the upper threshold of the mask length. It can be used when an IP *address/prefix* length is specified.

Parameter	Description
	If **ge** *greater-equal-value* and **le** *less-equal-value* are not specified, the value of prefix length is the mask length. For IPv4: • *less-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. • If only **le** is configured, the mask ranges from *prefixlen* to *less-equal-value*. For IPv6: • *less-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128. • If only **le** is configured, the mask ranges from *prefixlen* to *less-equal-value*.

Example

- Configure the IPv4 prefix list named **p1** to permit only the routes with the mask length ranging from 8 to 16 on the network segment 35.0.0.0/8.

```
admin@Xorplus# set routing prefix-list ipv4-family p1 seq 1 permit prefix 35.0.0.0/8 ge 16
admin@Xorplus# commit
```

- Configure the IPv6 prefix list named **p2** to permit the routes with the mask length ranging from 32 to 64 bits.

```
admin@Xorplus# set routing prefix-list ipv6-family p2 seq 1 permit prefix ::/0 ge 32 le 64
admin@Xorplus# commit
```

set routing prefix-list description

The **set routing prefix-list description** command creates a description of an IPv4/IPv6 prefix list.

The **delete routing prefix-list description** command deletes the description of an IPv4/IPv6 prefix list.

Command Syntax

set routing prefix-list {ipv4-family <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>**} description <***string***>**

delete routing prefix-list {ipv4-family <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>**} description**

Parameter

Parameter	Description
<*ip4-prefix-name*>	Specifies the name of an IPv4 prefix list.
<*ip6-prefix-name*>	Specifies the name of an IPv6 prefix list.
description <*string***>**	Optional. Specifies the description of an IPv4 prefix list. The value is a string.

Example

- Configure the description of the IP prefix list **p1**.

```
admin@Xorplus# set routing prefix-list ipv4-family p1 description Net1Pref
admin@Xorplus# commit
```

set routing community-list expanded

The **set routing community-list expanded** command defines a new expanded community list. The expanded community is only used to filter.

The **delete routing community-list expanded** command removes the expanded community list configuration.

Command Syntax

set routing community-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

delete routing community-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<*regular-expression*>	Specifies a string expression of communities attribute. It can be a regular expression (BGP Regular Expressions) to match the communities attribute in BGP updates. Space is not supported.

Example

- Configure a new expanded community list.

```
admin@Xorplus# set routing community-list expanded Comm1 permit regex 100:100
admin@Xorplus# commit
```

set routing community-list standard

The **set routing community-list standard** command configures a standard community list to match a specific community number attribute. Community-list is a named list of regular expressions. They are used to match the community number attributes in the routes for inclusion in, or exclusion from route policies.

The **delete routing community-list standard** command removes the standard community list configuration.

Command Syntax

set routing community-list standard <*community-list-name*> **{deny|permit} [local-as|no-advertise|no-export|internet|community** <*community*>**]**

delete routing community-list standard <*community-list-name*>**{deny|permit} [local-as|no-advertise|no-export|internet|community** <*community*>**]**

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
{local-as|no-advertise|no-export|internet|community <*community-numer*>**}**	Optional. Specifies BGP community type, it can be one of following BGP communities: • **local-AS:** a BGP community that restricts routes to your confederation's sub-AS. • **no-advertise:** a BGP community that is not advertised to anyone. • **no-export:** a BGP community that is not advertised to the eBGP peer. • **internet:** a BGP community that matches all routes. • **community** <*community-numer*>: Specifies the community number. The value is in AA:NN format where AA and NN are ranging from 0 to 65535.

Usage Guidelines

The BGP community list can be either standard or expanded. The standard BGP community list is a pair of values (such as 100:100) that can be tagged on a specific prefix and advertised to other neighbors or applied on route ingress.

Example

- Here is an example of a standard community list filter:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# commit
```

set routing extcommunity-list expanded

The **set routing extcommunity-list expanded** command defines a new expanded extcommunity-list.

The **delete routing extcommunity-list expanded** command removes the expanded community list configuration.

Command Syntax

set routing extcommunity-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

delete routing extcommunity-list expanded<*community-list-name*> **{deny|permit} regex** <*regular-expression*>

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<*regular-expression*>	Specifies a string expression of communities attribute. It can be a regular expression (BGP Regular Expressions) to match the communities attribute in BGP updates. The expanded community is only used to filter.

Example

- Define a new expanded extcommunity-list.

```
admin@Xorplus# set routing extcommunity-list expanded EXTcom1 permit regex 200:200
admin@Xorplus# commit
```

set routing extcommunity-list standard

The **set routing extcommunity-list standard** command defines a new standard extcommunity-list.

The **delete routing extcommunity-list standard** command removes the standard community list configuration.

Command Syntax

set routing extcommunity-list standard <*community-list-name*> **{deny|permit} {rt|soo} extcommunity** <*extcommunity*>

delete routing extcommunity-list standard <*community-list-name*> **{deny|permit} {rt|soo} extcommunity** <*extcommunity*>

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
{rt|soo}	**rt**: Indicates the Route Target value. **soo**: Indicates the Site of Origin.
<*extcommunity*>	Specifies an extended community value. The value is in the format of *as-number:nn* or *ipv4-address:nn*, where *as-number* is an integer with a range from 0 to 65535, and *nn* is also an integer.

Usage Guidelines

We can define multiple extcommunity-list under same name. In that case match will happen user defined order. Once the extcommunity-list matches to extended communities attribute in BGP updates it return permit or deny based upon the extcommunity-list definition. When there is no matched entry, deny will be returned. When *extcommunity* is empty it matches to any routes.

Example

- Define a new standard extcommunity-list.

```
admin@Xorplus# set routing extcommunity-list standard EXTcom1 permit rt extcommunity 100:100
admin@Xorplus# commit
```

set routing route-map set-action large-community

The **set routing route-map set-action large-community** command modifies the large community number to the existing community number attribute of the route.

The **delete routing route-map set-action large-community** command restores the default behavior of not modifying the large community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name*> order <*NUMBER*> set-action large-community none

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community1 {**<*large-community*>| **additive**}

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community2 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community3 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community4 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community5 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community6 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community7 {**<*large-community*>| **additive}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community none**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community1**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community2**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community3**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community4**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community5**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community6**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community7**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
none	Indicates that all the community attributes of routes are deleted.
<*large-community*>	Specifies the community number.
additive	Indicates that existing community attributes can be added to routes. Note that: If the keyword **additive** is not set, the original extended community attribute is replaced.

Example

- Modify the large community number to the existing community number attribute of the route to 10:22:30.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action large-community large-community1 10:22:30
admin@Xorplus# commit
```

set routing route-map call

The **set routing route-map call** command calls to another route-map, after any Set Actions have been carried out. If the route-map called returns *deny* then processing of the route-map finishes and the route is denied, regardless of the Matching Policy or the Exit Policy. If the called route-map returns *permit*, then Matching Policy and Exit Policy govern further behaviour, as normal.
The **delete routing route-map call** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> call** *<route-map-statement>*

delete routing route-map *<route-map-name>* **order** *<NUMBER>* **call** *<route-map-statement>*

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
call *<route-map-statement>*	Specifies the name of the route map. Required.

Example

- Configure a route map entry that calls to another route-map.

```
admin@Xorplus# set routing route-map GlobalMap order 10 call LocalMap
admin@Xorplus# commit
```

set routing route-map description

The **set routing route-map description** command adds descriptions to a route-map entry.
The **delete routing route-map description** command removes descriptions to a route-map entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> description** <*string*>

delete routing route-map <*route-map-name*> ***order*** <*NUMBER*> **description** <*string*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
description <*string*>	Specifies descriptions to a route map. The value is a string.

Example

- Add descriptions to a route-map entry.

```
admin@Xorplus# set routing route-map GlobalMap order 10 description GlobalMap
admin@Xorplus# commit
```

set routing route-map match as-path

The **set routing route-map match as-path** command matches the AS path attribute of the route with one or more regular expressions in the AS path list.
The **delete routing route-map match as-path** command restores the default behavior of not matching the AS path attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match as-path** <*as-path-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match as-path** <*as-path-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
match as-path <*as-path-list*>	Specifies the name of the AS path list to match the AS path attribute of the route.

Example

- Configure a match clause in the route map to match the AS path list:

```
admin@Xorplus# set routing as-path-list Aslist permit regex _20_
admin@Xorplus# set routing route-map GlobalMap order 10 match as-path Aslist
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match community

The **set routing route-map match community** command matches the community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match community** command restores the default behavior of not matching the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match community** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match community** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community <*community-list*>	Specifies the name of the community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the community list:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match community-with-exact-match

The **set routing route-map match community-with-exact-match** command matches the community number attribute must match exactly with the expressions in the community-list. However, the order of the communities in the community-list is of no significance.
The **delete routing route-map match community-with-exact-match** command restores the default behavior of not matching the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match community-with-exact-match** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match community-with-exact-match** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community-with-exact-match <*community-list*>	Specifies the name of the community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the community list:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community-with-exact-match COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn default-route

The **set routing route-map match evpn default-route** command matches the EVPN default route with the one configured in the match clause.
The **delete routing route-map match evpn default-route** command restores the default behavior of not matching the EVPN default route of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn default-route**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn default-route**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match clause in the route map to match the EVPN default route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn default-route
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn route-type

The **set routing route-map match evpn route-type** command matches the EVPN route-type with the one configured in the match clause.
The **delete routing route-map match evpn route-type** command restores the default behavior of not matching the EVPN route-type of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn route-type <macip|prefix|multicast>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn route-type <macip|prefix|multicast>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
route-type <macip|prefix|multicast>	Specifies the EVPN route type.

Example

- Configure a match clause in the route map to match the EVPN route-type:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn route-type macip
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn vni

The **set routing route-map match evpn vni** command matches the EVPN VNI ID with the one configured in the match clause.
The **delete routing route-map match evpn vni** command restores the default behavior of not matching the EVPN VNI ID of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn vni <***vni-id***>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn vni** <*vni-id*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
vni <*vni-id*>	Specifies the EVPN VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure a match clause in the route map to match the EVPN VNI ID:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn vni 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match extcommunity

The **set routing route-map match extcommunity** command matches the extended community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match extcommunity** command restores the default behavior of not matching the extended community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match extcommunity** <*extcommunity-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match extcommunity** <*extcommunity-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
extcommunity <*extcommunity-list*>	Specifies the name of the extended community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the extended community list:

```
admin@Xorplus# set routing extcommunity-list standard EXTcom1 permit 20
admin@Xorplus# set routing route-map GlobalMap order 10 match extcommunity EXTcom1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map matching-policy

The **set routing route-map matching-policy** command configures a route map entry with the given name and action by taking the CLI in the route map context. All route map entries with the same name belong to the same route map. The route map entry rules are processed in order by sequence number, until a match is found.
The **delete routing route-map matching-policy** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> matching-policy <deny|permit>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **matching-policy <deny|permit>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
matching-policy <deny|permit>	Specifies whether the route is available for further processing when there is a match. Required.

Example

- Configure a route map matching-policy.

```
admin@Xorplus# set routing route-map GlobalMap order 1 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match interface

The **set routing route-map match interface** command matches the outgoing VLAN interface value of the route with the value configured in the match clause.
The **delete routing route-map match interface** command restores the default behavior of not matching the outgoing VLAN interface value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match interface** <*interface*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match interface** <*interface*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
interface <*interface*>	Specifies the value to be matched with the outgoing VLAN interface of the route entry.

Example

- Configure a match clause in the route map to match the outgoing interface of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match interface vlan100
admin@Xorplus# commit
```

set routing route-map match ipv4-addr address

The **set routing route-map match ipv4-addr address** command matches the destination IP address prefix length or the prefix list of the routes.
The **delete routing route-map match ipv4-addr address** command restores the default behavior of not matching the destination IP address prefix length or the prefix list of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr address {prefix-len** <*prefix-len*>|**prefix-list** <*prefix-list-v4*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr address {prefix-len** <*prefix-len*>**|prefix-list** <*prefix-list-v4*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-len <*prefix-len*>	Specifies the prefix length to be matched. The value is an integer that ranges from 0 to 32.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the address prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr address prefix-len 24
admin@Xorplus# commit
```

set routing route-map match ipv4-addr next-hop

The **set routing route-map match ipv4-addrnext-hop** command matches the next-hop address prefix length or prefix list of the routes.
The **delete routing route-map match ipv4-addr next-hop** command restores the default behavior of not matching the next-hop address prefix length or prefix list of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr next-hop {prefix-len** <*prefix-len*>**|prefix-list** <*prefix-list-v4*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr next-hop {prefix-len** <*prefix-len*>**|prefix-list** <*prefix-list-v4*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-len <*prefix-len*>	Specifies the prefix length to be matched. The value is an integer that ranges from 0 to 32.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the next hop prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr next-hop prefix-len 24
admin@Xorplus# commit
```

set routing route-map match ipv4-addr route-source

The **set routing route-map match ipv4-addr route-source** command matches the source IP address prefix of the routes with one or more addresses in the prefix list.
The **delete routing route-map match ipv4-addr route-source** command restores the default behavior of not matching the source IP address prefix of the routes to their default value.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr route-source prefix-list** <*prefix-list-v4*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr route-source prefix-list** <*prefix-list-v4*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
<*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the source IP address prefix list P1.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr route-source prefix-list P1
admin@Xorplus# commit
```

set routing route-map match ipv6-addr

The **set routing route-map match ipv6-addr** command matches the destination IPv6 address or the next hop of the routes.
The **delete routing route-map match ipv6-addr** command restores the default behavior of not matching the destination IPv6 address or the next hop of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv6-addr {address prefix-list** <*prefix-list*> | **next-hop** <*next-hop-address*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv6-addr {address prefix-list** <*prefix-list*> | **next-hop** <*next-hop-address*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.
next-hop <*next-hop-address*>	Specifies the next hop address of the routes to be matched.

Example

- Configure a match clause in the route map to match the address prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv6-addr address next-hop ::ac12
admin@Xorplus# commit
```

set routing route-map match large-community

The **set routing route-map match large-community** command matches the BGP Large Community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match large-community** command restores the default behavior of not matching the BGP Large Community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match large-community** <*large-community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match large-community** <*large-community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
large-community <*large-community-list*>	Specifies the name of the BGP Large Community list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the BGP Large Community list:

```
admin@Xorplus# set routing large-community-list standard Largecom1 permit large-community 6215:22:33
admin@Xorplus# set routing route-map GlobalMap order 10 match large-community Largecom1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match local-preference

The **set routing route-map match local-preference** command matches the local preference value of the route with the value configured in the match clause.
The **delete routing route-map match local-preference** command restores the default behavior of not matching the local preference value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match local-preference** <*value*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match local-preference** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
local-preference <*value*>	Specifies the value to be matched with the route entry local preference in the range of 1 to 4294967295.

Example

- Configure a match clause in the route map to match the local preference of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match local-preference 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-action permit
admin@Xorplus# commit
```

set routing route-map match metric

The **set routing route-map match metric** command matches the MED value of the route with the value configured in the match clause.
The **delete routing route-map match metric** command restores the default behavior of not matching the MED value of the route.

Command Syntax

set routing route-map <*route-map-name***> order** <*NUMBER*> **match metric** <*value*>

delete routing route-map <*route-map-name*> **order <***NUMBER***> match metric** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric <*value*>	Specifies the value to be matched with the route entry MED in the range of 1 to 4294967295.

Example

- Configure a match clause in the route map to match the metric of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match metric 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match origin

The **set routing route-map match origin** command matches the route origin attribute of the route with route configured in the match clause.
The **delete routing route-map match origin** command restores the default behavior of not matching the route origin attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match origin <egp|igp|incomplete>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match origin <egp|igp|incomplete>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
origin <egp|igp|incomplete>	Specifies if the route origin attribute is matched with a match clause which originated as IGP, EGP, or has unknown origin. The unknown origin is typically redistributed from another routing protocol.

Example

- Configure a match clause in the route map to match the origin:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match origin egp
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match peer

The **set routing route-map match peer** command matches the peer ip address. This is a BGP specific match command.
The **delete routing route-map match peer** command restores the default behavior of not matching the peer ip address if the BGP neighbor of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match peer {ipv4-addr** <*ipv4-address*>**|ipv6-addr** <*ipv6-address*> | **local}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match peer {ipv4-addr** <*ipv4-address*>|**ipv6-addr** <*ipv6-address*> | **local}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
peer {ipv4-addr <*ipv4-address*>|**ipv6-addr** <*ipv6-address*>|**local}**	Specifies if the peer ip address if the BGP neighbor is matched with a match clause.

Example

- Configure a match clause in the route map to match the peer ip address if the BGP neighbor:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match peer ipv4-addr 100.100.100.1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match source-protocol

The **set routing route-map match source-protocol** command matches the source routing protocol value of the route with the value configured in the match clause.
The **delete routing route-map match source-protocol** command restores the default behavior of not matching the source routing protocol value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>	Specifies the bgp, connected, ospf, kernel, system or static value to be matched with the route entry source protocol.

Example

- Configure a match clause in the route map to match the source routing protocol value:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match source-protocol bgp
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match source-vrf

The **set routing route-map match source-vrf** command matches the source VRF attribute of the route with route configured in the match clause.
The **delete routing route-map match source-vrf** command restores the default behavior of not matching the source VRF attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match source-vrf** <*source-vrf*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match source-vrf** <*source-vrf*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
source-vrf <*source-vrf*>	Specifies if the source VRF attribute is matched with a match clause.

Example

- Configure a match clause in the route map to match the source VRF:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match source-vrf VRF-east
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match tag

The **set routing route-map match tag** command matches the tag value of the route with the one configured in the match clause. Applies to static routes that will be redistributed to ospfv2 and ospfv3 protocols.
The **delete routing route-map match tag** command restores the default behavior of not matching the tag value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match tag** <*value*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match tag** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
tag <*value*>	Numeric value to match with the route tag that ranges from 0 to 65535. Required.

Example

- Configure a match clause in the route map to match the tag value:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match tag 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map on-match

The **set routing route-map on-match** command specifies an alternative Exit Policy to take if the entry matched, rather than the normal policy of exiting the route-map and permitting the route.
The **delete routing route-map on-match** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> on-match {goto <***NUMBER2***>| next}**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* **on-match {goto <***NUMBER2***>| next}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
{goto <*NUMBER2***>| next}**	The two possibilities are: • **next**: Continue on with processing of the route-map entries. • **goto <***NUMBER2***>**: Jump ahead to the first route-map entry whose order in the route-map is >=NUMBER2. Jumping to a previous entry is not permitted. The value is an integer that ranges from 1 to 65535.

Example

- Configure a on-match clause in the route map:

```
admin@Xorplus# set routing route-map GlobalMap order 10 on-match next
admin@Xorplus# commit
```

set routing route-map set-action aggregator

The **set routing route-map set-action aggregator** command is a complement to the ATOMIC_AGGREGATE attribute where routing information is missing - it contains the AS number that initiated the route aggregation and the IP address of the BGP publisher that formed the aggregated route.

The **delete routing route-map set-action aggregator** command removes the configurations.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action aggregator {as** <*as-number*>|**ip** <*ipv4-address*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action aggregator {as** <*as-number*>|**ip** <*ipv4-address*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
as <*as-number*>	Specifies the AS number that initiated the route aggregation. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.
ip <*ipv4-address*>	Specifies the IPv4 address of the BGP publisher that formed the aggregated route.

Usage Guidelines

ATOMIC_AGGREGATE is a warning that routing information is missing, and the AGGREGATOR attribute complements where routing information is missing - it contains the AS number that initiated the route aggregation and the IP address of the BGP publisher that formed the aggregated route. When performing route aggregation, the AGGREGATOR attribute is added at the same time as the ATOMIC-AGGREGATE attribute for the aggregated route information.

Example

- Configure the ATOMIC_AGGREGATE attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action aggregator as 100
admin@Xorplus# commit
```

set routing route-map set-action as-path exclude

The **set routing route-map set-action as-path exclude** command removes all occurrences of the configured AS Path from the AS Path attribute of the route.
The **delete routing route-map set-action as-path exclude** command restores the default behavior of not modifying the AS Path attribute list.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action as-path exclude** <*AS*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action as-path exclude** <*AS*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
as-path exclude <*AS*>	Specifies the AS number to be removed from the AS Path attribute of the route. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example

- Configure a action clause in the route map to remove the AS from the AS Path attribute of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action as-path exclude 10
admin@Xorplus# commit
```

set routing route-map set-action as-path prepend

The **set routing route-map set-action as-path prepend** command prepends the list of the configured AS numbers to the AS Path attribute of the routes. To ensure that the AS path conforms to standards, the local AS is prepended after this command is executed.
The **delete routing route-map set-action as-path prepend** command restores the default behavior of not modifying the AS Path attribute list.

NOTE: The **delete** form of the command deletes the entire list of AS-Path prepend configuration regardless of the parameter list.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action as-path prepend [as1** <*AS*> | **as2** <*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action as-path prepend [as1**<*AS*> | **as2**<*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prepend [as1<*AS*> | **as2**<*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]	Specifies the AS numbers to be prepended from the AS Path attribute of the route. At most six AS number can be set. The value of <*AS*> is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example

- Configure a action clause in the route map to prepend the AS from the AS Path attribute of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action as-path prepend as1 102
admin@Xorplus# commit
```

set routing route-map set-action atomic-aggregate

The **set routing route-map set-action atomic-aggregate** command is used to inform the route recipient that the route is aggregated and is a recognized optional attribute.

The **delete routing route-map set-action atomic-aggregate** command removes the configurations.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action atomic-aggregate**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action atomic-aggregate**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.

Usage Guidelines

Sometimes a BGP publisher will receive two overlapping routes, one of which contains addresses that are a subset of the other route. Normally the BGP publisher prefers the finer route (the former), but when publishing externally, if it chooses to publish the coarser one (the latter), it then needs to append the ATOMIC-AGGREGATE attribute to inform the peer. It is actually a warning, because publishing the coarser route means that the finer routing information is lost in the publishing process. When performing route aggregation, the ATOMIC-AGGREGATE attribute is added to the aggregated route information.

Example

- Configure a action clause to inform the route recipient that the route is aggregated and is a recognized optional attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action atomic-aggregate
admin@Xorplus# commit
```

set routing route-map set-action comm-list-delete

The **set routing route-map set-action comm-list-delete** command removes communities value from BGP communities attribute.

When BGP route's communities value matches to the community list name, the communities value is removed. When all of communities value is removed eventually, the BGP update's communities attribute is completely removed.

The **delete routing route-map set-action comm-list-delete** command restores the default behavior of not deleting the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action comm-list-delete** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action comm-list-delete** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
comm-list-delete<*community-list*>	Specifies the name of the community-list.

Example

- Configure to remove communities value from BGP communities attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action comm-list-delete Comlst
admin@Xorplus# commit
```

set routing route-map set-action community

The **set routing route-map set-action community** command changes the community number to the existing community number attribute of the route.

The **delete routing route-map set-action community** command restores the default behavior of not changing the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action community** <*community*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action community** <*community*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community <*community*>	Specifies the community number.

Example

- Add the community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action community 11:101
admin@Xorplus# commit
```

set routing route-map set-action community-additive

The **set routing route-map set-action community-additive** command adds the community number to the existing community number attribute of the route.

The **delete routing route-map set-action community-additive** command restores the default behavior of not adding the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action community-additive** <*community*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action community-additive** <*community*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community-additive <*community*>	Specifies the community number.

Example

- Add the community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action community-additive 11:101
admin@Xorplus# commit
```

set routing route-map set-action extcommunity

The **set routing route-map set-action extcommunity** command modifies the extended community number to the existing community number attribute of the route.

The **delete routing route-map set-action extcommunity** command restores the default behavior of not modifying the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity1** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity2** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity3** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity4** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity5** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity6** *<extcommunity>*

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity7** *<extcommunity>*

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity1**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity2**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity3**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity4**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity5**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity6**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* ***set-action*** **extcommunity <rt|soo> extcommunity7**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
rt	Indicates the route-target extended community.
soo	Indicates the Site of Origin value.
<extcommunity>	Specifies the community number.

Example

- Modify the extended community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity rt extcommunity1 100:2
admin@Xorplus# commit
```

set routing route-map set-action extcommunity bandwidth

The **set routing route-map set-action extcommunity bandwidth** command sets the BGP link-bandwidth extended community for the prefix (best path) for which it is applied.

The **delete routing route-map set-action extcommunity bandwidth** command restores the default behavior of not modifying the BGP link-bandwidth extended community of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity bandwidth {<***bandwidth***>|cumulative|num-multipaths}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action extcommunity bandwidth {**<*bandwidth*>**|cumulative|num-multipaths}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
<*bandwidth***>|cumulative|num-multipaths**	The link-bandwidth can be specified as an explicit value (specified in Mbps), or the router can be told to use the cumulative bandwidth of all multipaths for the prefix or to compute it based on the number of multipaths.

Example

- The following command examples show how you can set the BGP link bandwidth extended community against all prefixes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity bandwidth num-multipaths
admin@Xorplus# commit
```

set routing route-map set-action extcommunity bandwidth-non-transitive

The **set routing route-map set-action extcommunity bandwidth-non-transitive** command sets link bandwidth extended community as non-transitive. The link bandwidth extended community is encoded as transitive unless the set command explicitly configures it as non-transitive.

The **delete routing route-map set-action extcommunity bandwidth-non-transitive** command restores the default behavior of not modifying the BGP link-bandwidth extended community of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity bandwidth-non-transitive** <*bandwidth*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action extcommunity bandwidth-non-transitive** <*bandwidth*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
<*bandwidth***>**	The link-bandwidth can be specified as an explicit value (specified in Mbps).

Example

- The following command examples sets link bandwidth extended community as non-transitive.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity bandwidth-non-transitive 128
admin@Xorplus# commit
```

set routing route-map set-action ip-next-hop

The **set routing route-map set-action ip-next-hop** command sets the IP address of the next-hop address or peer address of the route with the value configured in the action clause or keep unchanged.
The **delete routing route-map set-action ip-next-hop** command restores the default behavior of not modifying the IP address of the next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ip-next-hop {ipv4-addr** <*next-hop-address*> | **peer-address | unchanged}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action ip-next-hop {ipv4-addr** <*next-hop-address*> | **peer-address | unchanged}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
ip-next-hop {ipv4-addr <*next-hop-address*>	**peer-address	unchanged}**	Specifies the IPv4 address to be set as the next-hop address or peer address of the route or keep unchanged.

Example

- Set the IP address of the next-hop of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ip-next-hop ipv4-addr 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action ipv4-vpn-next-hop

The **set routing route-map set-action ipv4-vpn-next-hop** command sets the IP address of the VPN next-hop of the route with the value configured in the action clause.
The **delete routing route-map set-action ipv4-vpn-next-hop** command restores the default behavior of not modifying the IP address of the VPN next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ipv4-vpn-next-hop** <*next-hop-address*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action ipv4-vpn-next-hop** <*next-hop-address*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
ipv4-vpn-next-hop <*next-hop-address*>	Specifies the IPv4 address to be set as the VPN next-hop address of the route.

Example

- Set the IP address of the VPN next-hop of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ipv4-vpn-next-hop 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action ipv6-next-hop

The **set routing route-map set-action ipv6-next-hop** command sets the IP address of the next-hop address or peer address of the route with the value configured in the action clause or keep unchanged.
The **delete routing route-map set-action ipv6-next-hop** command restores the default behavior of not modifying the IP address of the next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ipv6-next-hop {[global ipv6-addr** <*next-hop-address*>] | [**local ipv6-addr** <*next-hop-address*>] | **peer-address | prefer-global}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action ipv6-next-hop {[global ipv6-addr** <*next-hop-address*>**] | [local ipv6-addr** <*next-hop-address*>**] | peer-address | prefer-global}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
{[global ipv6-addr <*next-hop-address*>] | [**local ipv6-addr** <*next-hop-address*>] | **peer-address | prefer-global}**	Specifies the IPv6 address to be set as the next-hop address or peer address of the route .

Example

- Set the IP address of the peer address of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ipv6-next-hop peer-address
admin@Xorplus# commit
```

set routing route-map set-action label-index

The **set routing route-map set-action label-index** command modifies the label-index attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action label-index** command restores the default behavior of not modifying the label-index attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action label-index** <*label-index*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action label-index** <*label-index*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
label-index <*label-index*>	Specifies the label index value to be set in the route entry. Range: 0 to 1048560.

Example

- Configure a action clause in the route map to modify the label-index value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action label-index 100
admin@Xorplus# commit
```

set routing route-map set-action large-comm-list-delete

The **set routing route-map set-action large-comm-list-delete** command removes communities value from BGP large communities attribute.

When BGP route's communities value matches to the large community list name, the communities value is removed. When all of large communities value is removed eventually, the BGP update's large communities attribute is completely removed.

The **delete routing route-map set-action large-comm-list-delete** command restores the default behavior of not deleting the large community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-comm-list-delete** *<large-community-list>*

delete routing route-map *<route-map-name>* **order** *<NUMBER>* **set-action large-comm-list-delete** *<large-community-list>*

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
large-comm-list *<large-community-list>*	Specifies the name of the large-community-list.

Example

- Configure to remove communities value from BGP large communities attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action large-comm-list-delete LargeComlst
admin@Xorplus# commit
```

set routing route-map set-action local-preference

The **set routing route-map set-action local-preference** command modifies the local-preference attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action local-preference** command restores the default behavior of not modifying the local-preference attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action local-preference** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action local-preference** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
local-preference <*VALUE*>	Specifies the value to be set as the local-preference attribute of the route entry. Range: 0 to 4294967295.

Example

- Configure a action clause in the route map to modify the local-preference value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action local-preference 100
admin@Xorplus# commit
```

set routing route-map set-action metric

The **set routing route-map set-action metric** command modifies the metric attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action metric** command restores the default behavior of not modifying the metric attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action metric** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action metric** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric <*VALUE*>	Specifies the value to be set as the metric attribute of the route entry. Range: 0 to 4294967295.

Example

- Configure a action clause in the route map to modify the metric value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action metric 100
admin@Xorplus# commit
```

set routing route-map set-action metric-type

The **set routing route-map set-action metric-type** command modifies the metric-type attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action metric-type** command restores the default behavior of not modifying the metric-type attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action metric-type <type-1|type-2>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action metric-type <type-1|type-2>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric-type <type-1|type-2>	Specifies the metric-type value of the route entry. The value could be **type-1** or **type-2**.

Example

- Configure a action clause in the route map to modify the metric-type value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action metric-type type-1
admin@Xorplus# commit
```

set routing route-map set-action origin

The **set routing route-map set-action origin** command modifies the origin attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action origin** command restores the default behavior of not modifying the origin attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action origin <egp|igp|incomplete>**

delete routing route-map <*route-map-name*>**order** <*NUMBER*> **set-action origin <egp|igp|incomplete>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
origin <egp|igp|incomplete>	Selects the route update originated to IGP, EGP, or incomplete. When incomplete is selected, the route update origin is set to unknown.

Example

- Configure a action clause in the route map to modify the origin value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action origin egp
admin@Xorplus# commit
```

set routing route-map set-action originator-id

The **set routing route-map set-action originator-id** command modifies the originator-id attribute of the BGP route entry with the value configured in the action clause.
The **delete routing route-map set-action originator-id** command restores the default behavior of not modifying the originator-id attribute of the BGP route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action originator-id** <*ipv4-address*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action originator-id** <*ipv4-address*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
originator-id <*ipv4-address*>	Specifies originator-id attribute of the BGP route entry. The value is an IPv4 address.

Example

- Configure a action clause in the route map to modify the originator-id attribute of the BGP route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action originator-id 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action src

The **set routing route-map set-action src** command sets the preferred source address for matching routes when installing in the kernel.
The **delete routing route-map set-action src** command restores the default behavior of not modifying the source address of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action src {ipv4-addr** <*ipv4-address*>| **ipv6-addr** <*ipv6-address*>**}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action src {ipv4-addr** <ipv4-address>| **ipv6-addr**<ipv6-address>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
src {ipv4-addr <*ipv4-address*>| **ipv6-addr** <*ipv6-address*>**}**	Specifies the preferred source address to be set for a route.

Example

- Configure a action clause in the route map to modify the source address of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action src ipv4-addr 100.100.100.1
admin@Xorplus# commit
```

set routing route-map set-action tag

The **set routing route-map set-action tag** command modifies the tag value of the route with the one configured in the action clause. Applicable to static routes that will be redistributed to ospfv2 and ospfv3 protocols.
The **delete routing route-map set-action tag** command removes the action clause tag value.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action tag** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action tag** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
tag <*VALUE*>	Numeric value to change the route entry tag. Range: 0-65535. Required.

Example

- Configure a action clause in the route map to modify the tag value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action tag 100
admin@Xorplus# commit
```

set routing route-map set-action weight

The **set routing route-map set-action weight** command modifies the weight value of the route with the one configured in the action clause.
The **delete routing route-map set-action weight** command restores the default behavior of not modifying the weight attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order** <*NUMBER*>**set-action weight** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action weight** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
weight <*VALUE*>	Specifies the value to be set as the weight attribute of the route. Range: 0 to 65535.

Example

- Configure a action clause in the route map to modify the weight value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action weight 100
admin@Xorplus# commit
```

Route Leaking Commands

- BGP Route Leaking Commands
  - set protocols bgp ipv4-unicast import vrf
  - set protocols bgp ipv6-unicast import vrf
  - set protocols bgp ipv6-unicast import vrf-route-map
  - set protocols bgp vrf ipv4-unicast import vrf
  - set protocols bgp vrf ipv4-unicast import vrf-route-map
  - set protocols bgp vrf ipv6-unicast import vrf
- Static Route Leaking Commands
  - set protocols static route nexthop-vrf next-hop
  - set protocols static vrf route nexthop-vrf next-hop

BGP Route Leaking Commands

- set protocols bgp ipv4-unicast import vrf
- set protocols bgp ipv6-unicast import vrf
- set protocols bgp vrf ipv4-unicast import vrf
- set protocols bgp vrf ipv4-unicast import vrf-route-map
- set protocols bgp vrf ipv6-unicast import vrf

set protocols bgp ipv4-unicast import vrf

Run the command **set protocols bgp ipv4-unicast import vrf** to configure route leaking by importing BGP routes from the specified user defined non-default VRF into the default VRF.

Run the command **delete protocols bgp ipv4-unicast import vrf** to remove this configuration from the switch database.

Command Syntax

set protocols bgp ipv4-unicast import vrf <*vrf-name***>**

delete protocols bgp ipv4-unicast import vrf <*vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF from which routes are imported. This is the destination VRF for the route and it must be a non-default user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP routes from vrf2 into the default VRF.

```
admin@Xorplus# set protocols bgp ipv4-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp ipv6-unicast import vrf

Run the command **set protocols bgp ipv6-unicast import vrf** to configure route leaking by importing IPv6 unicast routes from a user defined non-default VRF into the specified user defined VRF.

Run the command **delete protocols bgp ipv6-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp ipv6-unicast import vrf <*vrf-name***>**

delete protocols bgp ipv6-unicast import vrf <*vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF from which routes are imported. This is must be a non-default user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP IPv6 routes from vrf2 into the default VRF.

```
admin@Xorplus# set protocols bgp ipv6-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp ipv6-unicast import vrf-route-map

Run the command **set protocols bgp ipv6-unicast import vrf-route-map** to specify a route map to filter IPv6 routes when importing routes from one VRF into another VRF. This command is useful to control the number of routes leaked between two VRFs using BGP. The conditions for which routes needs to be leaked and which routes should be excluded are specified in the route map and then applied when importing the routes. The optional parameter **vrf** is used to specify the VRF to which the routes are imported after filtering. If VRF is not specified then routes are imported into the default VRF.

Run the command **delete set protocols bgp ipv6-unicast import vrf-route-map** to delete this configuration from the switch database.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] ipv6-unicast import vrf-route-map <***map-name***>**

delete protocols bgp [vrf <*vrf-name***> ipv6-unicast import vrf-route-map**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Optional. Specifies the VRF name to which routes will be imported. The value is a string.
vrf-route-map <*map-name***>**	Specifies the name of the route map to apply when importing routes to a VRF. The value is a string.

Example

- This example applies route map *map1* when importing IPv6 routes into the default VRF.

```
admin@Xorplus# set protocols bgp ipv6-unicast import vrf-route-map map1
admin@Xorplus# commit
```

set protocols bgp vrf ipv4-unicast import vrf

Run the command **set protocols bgp vrf ipv4-unicast import vrf** to establish route leaking by importing IPv4 unicast routes from one VRF into another VRF.

Please note that the source VRF, to which the routes are imported to from the destination VRF must be a non-default VRF in this case. The destination VRF, from which the routes are imported can be a user defined non-default VRF or it could be the default VRF.

Run the command **delete protocols bgp vrf ipv4-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp vrf <*vrf-name***> ipv4-unicast import vrf <***vrf-name* **| default>**

delete protocols bgp vrf <*vrf-name***> ipv4-unicast import vrf <***vrf-name* **| default>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route and it must be a non-default user defined VRF. The value is a string.
vrf <*vrf-name* **| default>**	Specifies the destination VRF, it could be the default VRF or the user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP IPv4 routes from vrf2 into vrf1.

```
admin@Xorplus# set protocols bgp vrf vrf1 ipv4-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp vrf ipv4-unicast import vrf-route-map

Run the command **set protocols bgp ipv4-unicast import vrf-route-map** to specify a route map to filter IPv4 routes when importing routes from one VRF into another VRF. This command is useful to control the number of routes leaked between two VRFs using BGP. The conditions for which routes needs to be leaked and which routes should be excluded are specified in the route map and then applied when importing the routes. The optional parameter **vrf** is used to specify the VRF to which the routes are imported after filtering. If VRF is not specified then routes are imported into the default VRF.

Run the command **delete set protocols bgp ipv4-unicast import vrf-route-map** to delete this configuration from the switch database.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] ipv4-unicast import vrf-route-map <***map-name***>**

delete protocols bgp [vrf <*vrf-name***> ipv4-unicast import vrf-route-map**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Optional. Specifies the VRF name to which routes will be imported. The value is a string.
vrf-route-map <*map-name***>**	Specifies the name of the route map to apply when importing routes to a VRF. The value is a string.

Example

- This example applies route map *map1* when importing routes into the default VRF.

```
admin@Xorplus# set protocols bgp ipv4-unicast import vrf-route-map map1
admin@Xorplus# commit
```

set protocols bgp vrf ipv6-unicast import vrf

Run the command **set protocols bgp vrf ipv6-unicast import vrf** to enable route leaking by importing BGP IPv6 routes from the user defined or default VRF into the specified user defined non-default VRF.

Run the command **delete protocols bgp vrf ipv6-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp vrf <*vrf-name****> ipv6-unicast import vrf <****vrf-name*** **| default>**

delete protocols bgp vrf <*vrf-name****> ipv6-unicast import vrf <****vrf-name*** **| default>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the source VRF name for the imported IPv6 BGP route. This is the source VRF for the route and it must be a non-default user defined VRF. The value is a string.
vrf <*vrf-name* **| default>**	Specifies the destination VRF from which the routes are imported, it could be the default VRF or a user defined VRF. The value is a string.

Example

- This example configures route leaking by importing routes from vrf2 into vrf1.

```
admin@Xorplus# set protocols bgp vrf vrf1 ipv6-unicast import vrf vrf2
admin@Xorplus# commit
```

Static Route Leaking Commands

- set protocols static vrf route nexthop-vrf next-hop
- set protocols static route nexthop-vrf next-hop

set protocols static route nexthop-vrf next-hop

Run the command **set protocols static route nexthop-vrf next-hop** to configure a static leak route in the default VRF. The source VRF for the route is the default VRF and the destination next-hop router is in the specified next-hop VRF.

To delete this route, run the command **delete protocols static route nexthop-vrf.**

Command Syntax

set protocols static route <*IPv4Net* | *IPv6Net***> nexthop-vrf <***vrf-name***> next-hop <***IPv4* | *IPv6***>**

set protocols static route <*IPv4Net* | *IPv6Net***> nexthop-vrf <***vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route.
route <*IPv4Net*	*IPv6Net***>**	Specifies the IPv4 or IPv6 network prefix, e.g. 10.0.0.0/24.
nexthop-vrf <*vrf-name***>**	Specifies the next-hop VRF for the static route. This is the destination VRF.
next-hop <*IPv4*	*IPv6***>**	Specifies the next-hop IPv4 or IPv6 router address in the destination VRF.

Usage Guidelines

Please note that if the route prefix chosen is an IPv4 network prefix then the next-hop router address in the next-hop VRF must also be an IPv4 address. Similarly, if the route prefix is an IPv6 network prefix, then the next-hop router address in the next-hop VRF must also be an IPv6 address.

Example

- Configure the static route leak in the default VRF for which the destination VRF is vrf2.

```
admin@Xorplus# set protocols static route 10.5.5.0/24 nexthop-vrf vrf2 next-hop 10.6.6.6
admin@Xorplus# commit
```

set protocols static vrf route nexthop-vrf next-hop

Run the command **set protocols static vrf route nexthop-vrf next-hop** to configure a static leak route. The route is created in one VRF for which the next-hop router is located in a different VRF.

Run the command **delete protocols static vrf route** to delete this static route the switch configuration.

Command Syntax

set protocols static vrf <*vrf-name***> route <***IPv4Net* **|** *IPv6Net***> nexthop-vrf <***vrf-name* **| default> next-hop <***IPv4* | *IPv6***>**

delete protocols static vrf <*vrf-name***> route <***IPv4Net* | *IPv6Net***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route.
route <*IPv4Net*	*IPv6Net***>**	Specifies the IPv4 or IPv6 network prefix, e.g. 10.0.0.0/24.
nexthop-vrf <*vrf-name***| default>**	Specifies the next-hop VRF for the static route. This is the destination VRF.
next-hop <*IPv4*	*IPv6***>**	Specifies the next-hop IPv4 or IPv6 router address in the destination VRF.

Usage Guidelines

Please note that if the route prefix chosen is an IPv4 network prefix then the next-hop router address in the next-hop VRF must also be an IPv4 address. Similarly, if the next route prefix is an IPv6 network prefix, then the next-hop router address in the next-hop VRF must also be an IPv6 address.

Example

- Configure the static route leak in vrf1 for which the destination VRF is vrf2.

```
admin@Xorplus# set protocols static vrf vrf1 route 10.5.5.0/24 nexthop-vrf vrf2 next-hop 10.6.6.6
admin@Xorplus# commit
```

BFD Configuration Commands

- run show bfd
- run show bfd counters
- run show bfd peers
- set protocols bfd multihop peer local-address
- set protocols bfd multihop peer local-address detect-multiplier
- set protocols bfd multihop peer local-address minimum-ttl
- set protocols bfd multihop peer local-address passive-mode
- set protocols bfd multihop peer local-address receive-interval
- set protocols bfd multihop peer local-address shutdown
- set protocols bfd multihop peer local-address transmit-interval
- set protocols bfd peer detect-multiplier
- set protocols bfd peer echo-mode
- set protocols bfd peer echo receive-interval
- set protocols bfd peer echo transmit-interval
- set protocols bfd peer local-address
- set protocols bfd peer minimum-ttl
- set protocols bfd peer passive-mode
- set protocols bfd peer receive-interval
- set protocols bfd peer shutdown
- set protocols bfd peer transmit-interval
- set protocols bfd profile
- set protocols bfd profile detect-multiplier
- set protocols bfd profile echo-mode
- set protocols bfd profile echo receive-interval
- set protocols bfd profile echo transmit-interval
- set protocols bfd profile minimum-ttl
- set protocols bfd profile passive-mode
- set protocols bfd profile receive-interval
- set protocols bfd profile shutdown
- set protocols bfd profile transmit-interval
- set protocols bgp bfd
- set protocols ospf6 interface bfd
- set protocols ospf interface bfd
- set protocols pim interface bfd



run show bfd counters

The **run show bfd** command displays the counter informations about BFD sessions.

Command Syntax

run show bfd [**vrf** <*vrf-name*>] [**interface** <*interface*>] | **multihop**] ***peer*** <*peer-ip*> **counters**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[**interface** <*interface*>] | **multihop**]	Optional. • **interface** <*interface*>: Specifies an interface for BGP connection. • **multihop**: Shows informations about a multi-hop BFD session.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Example

• Show the counter information about the BFD session.

```
admin@Xorplus# run show bfd peer 1.1.1.1 counters
peer 1.1.1.1 local-address 1.1.1.2 vrf default
                Control packet input: 0 packets
                Control packet output: 1 packets
                Echo packet input: 0 packets
                Echo packet output: 0 packets
                Session up events: 0
                Session down events: 0
                Zebra notifications: 1
```

run show bfd peers

The **run show bfd peers** command displays informations about all the BFD sessions.

Command Syntax

run show bfd [**vrf** <*vrf-name*>] **peers [brief | counters]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[brief | counters]	Optional. • **brief**: Displays brief information about all the BFD sessions. • **counters**: Displays the counter information about all the BFD sessions.

Example

• Show information about all the BFD session.

```
admin@Xorplus# run show bfd peers
BFD Peers:
        peer 3.3.3.3 local-address 3.3.3.2 vrf vrf1 interface vlan100
                ID: 984327
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 20
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: 30ms
                        Echo transmission interval: 30ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled

        peer 3.3.3.3 local-address 3.3.3.2 vrf default interface vlan3
                ID: 3820553826
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: 10ms
                        Echo transmission interval: 10ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled

        peer 2.2.2.2 multihop local-address 2.2.2.3 vrf vrf1
                ID: 219448436
```

```
Remote ID: 0
Active mode
Minimum TTL: 254
Status: down
Downtime: 1 hour(s), 53 minute(s), 4 second(s)
Diagnostics: ok
Remote diagnostics: ok
Peer Type: configured
Local timers:
        Detect-multiplier: 3
        Receive interval: 300ms
        Transmission interval: 300ms
        Echo receive interval: 50ms
        Echo transmission interval: disabled
Remote timers:
        Detect-multiplier: 3
        Receive interval: 1000ms
        Transmission interval: 1000ms
        Echo receive interval: disabled
```

set protocols bfd multihop peer local-address

The **set protocols bfd multihop peer local-address** command creates a multi-hop BFD session and specifies the peer IP address.

The **delete protocols bfd multihop peer local-address** command deletes the multi-hop BFD session.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] ***peer*** <*peer-ip*> [**local-address** <*local-ip*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Optional. Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address. **Note:** This option is mandatory for IPv6.

Example

- Create a multi-hop BFD session to the peer IP address 2.2.2.2.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address detect-multiplier

The **set protocols bfd multihop peer local-address detect-multiplier** command configures the detection multiplier to determine packet loss for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for BFD peer 2.2.2.2 for a multi-hop BFD session.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address minimum-ttl

The **set protocols bfd multihop peer local-address minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of thightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address passive-mode

The **set protocols bfd multihop peer local-address passive-mode** command configures the BFD session as passive for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **passive-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peer before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid all the other nodes sending BFD control packets.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 passive-mode
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address receive-interval

The **set protocols bfd multihop peer local-address receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address shutdown

The **set protocols bfd multihop peer local-address shutdown** command can be used to disable the BFD peer. When the peer is disabled an 'administrative down' message is sent to the remote peer for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3shutdown
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address transmit-interval

The **set protocols bfd multihop peer local-address transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 transmit-interval 500
admin@Xorplus# commit
```

set protocols bfd peer detect-multiplier

The **set protocols bfd peer detect-multiplier** command configures the detection multiplier to determine packet loss for a single-hop BFD session.

The **delete protocols bfd peer detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for BFD peer 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd peer echo-mode

The **set protocols bfd peer echo-mode** command can be used to enable BFD echo mode for a single-hop BFD session. This mode is disabled by default.

The **delete protocols bfd peer echo-mode** command sets the configuration to the default value.

> **NOTEs:**
> - Echo function is only supported in single-hop BFD case.
> - BFD echo mode is incompatible with that on other vendors, that is, echo mode can work only between PICOS switches.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Usage Guidelines

It is recommended that the transmission interval of control packets to be increased after enabling echo-mode to reduce bandwidth usage. For example: transmit-interval 2000. Echo mode is not supported on multi-hop setups.

Example

- Enable BFD echo mode for BFD peer 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo-mode
admin@Xorplus# commit
```

set protocols bfd peer echo receive-interval

The **set protocols bfd peer echo receive-interval** command configures the minimum time interval between received BFD echo packets for a single-hop BFD session.

The **delete protocols bfd peer echo receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo receive-interval** [**<***receive-interval***> | disabled**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
echo receive-interva [**<***receive-interval***> | disabled**]	Specifies the minimum time interval between received BFD echo packets in milliseconds. The value **disabled** indicates that the switch does not support reception of BFD echo packets. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between received BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo receive-interval 60
admin@Xorplus# commit
```

set protocols bfd peer echo transmit-interval

The **set protocols bfd peer echo transmit-interval** command configures the minimum time interval between transmitted BFD echo packets for a single-hop BFD session.

The **delete protocols bfd peer echo transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
echo transmit-interval <*transmit-interval***>**	Specifies the minimum time interval between transmitted BFD echo packets in milliseconds. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between transmitted BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo transmit-interval 60
admin@Xorplus# commit
```

set protocols bfd peer local-address

The **set protocols bfd peer local-address** command creates a BFD session and specifies the peer IP address.

The **delete protocols bfd peer local-address** command delete the BFD session.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer*** <*peer-ip*> [**local-address** <*local-ip*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address. **Note:** This option is mandatory for IPv6.

Example

- Create a BFD session link to the peer IP address 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2
admin@Xorplus# commit
```

set protocols bfd peer minimum-ttl

The **set protocols bfd peer minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a single-hop BFD session.

The **delete protocols bfd peer minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of tightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd peer passive-mode

The **set protocols bfd peer passive-mode** command configures the BFD session as passive for a single-hop BFD session.

The **delete protocols bfd peer passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **passive-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peer before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid other nodes sending BFD control packets proactively.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 passive-mode
admin@Xorplus# commit
```

set protocols bfd peer receive-interval

The **set protocols bfd peer receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a single-hop BFD session.

The **delete protocols bfd peer receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd peer shutdown

The **set protocols bfd peer shutdown** command can be used to disable the BFD peer for a single-hop BFD session. When the peer is disabled an 'administrative down' message is sent to the remote peer.

The **delete protocols bfd peer shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 shutdown
admin@Xorplus# commit
```

set protocols bfd peer transmit-interval

The **set protocols bfd peer transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a single-hop BFD session.

The **delete protocols bfd peer transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 transmit-interval 500
admin@Xorplus# commit
```

set protocols bfd profile

The **set protocols bfd profile** command adds a new profile for OSPFv2/v3, BGP or PIM protocols to modify the BFD parameters.

The **delete protocols bfd profile** command deletes the profile.

Command Syntax

set protocols bfd profile <*profile-name*>

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Example

- Creates a BFD profile p2.

```
admin@Xorplus# set protocols bfd profile p2
admin@Xorplus# commit
```

set protocols bfd profile detect-multiplier

The **set protocols bfd profile detect-multiplier** command configures the detection multiplier to determine packet loss for a profile.

The **delete protocols bfd profile detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for profile p2.

```
admin@Xorplus# set protocols bfd profile p2 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd profile echo-mode

The **set protocols bfd profile echo-mode** command can be used to enable BFD echo mode for a profile. This mode is disabled by default.

The **delete protocols bfd profile echo-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **echo-mode**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Usage Guidelines

It is recommended that the transmission interval of control packets to be increased after enabling echo-mode to reduce bandwidth usage. For example: transmit-interval of 2000ms. Echo mode is not supported on multi-hop BFD sessions.

Example

- Enable BFD echo mode.

```
admin@Xorplus# set protocols bfd profile p2 echo-mode
admin@Xorplus# commit
```

set protocols bfd profile echo receive-interval

The **set protocols bfd profile echo receive-interval** command configures the minimum time interval between received BFD echo packets for a profile.

The **delete protocols bfd profile echo receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
echo receive-interva [**<***receive-interval***>	disabled**]	Specifies the minimum time interval between received BFD echo packets in milliseconds. The value **disabled** indicates that the switch does not support reception of BFD echo packets. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between received BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 echo receive-interval 60
admin@Xorplus# commit
```

set protocols bfd profile echo transmit-interval

The **set protocols bfd profile echo transmit-interval** command configures the minimum time interval between transmitted BFD echo packets for a profile.

The **delete protocols bfd profile echo transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
echo transmit-interval <*transmit-interval***>**	Specifies the minimum time interval between transmitted BFD echo packets in milliseconds. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between transmitted BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 echo transmit-interval 60
admin@Xorplus# commit
```

set protocols bfd profile minimum-ttl

The **set protocols bfd profile minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a profile.

The **delete protocols bfd profile minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of tightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd profile p2 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd profile passive-mode

The **set protocols bfd profile passive-mode** command configures the BFD session as passive for a profile.

The **delete protocols bfd profile passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **passive-mode**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peers before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid other BFD nodes sending control packets proactively.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd profile p2 passive-mode
admin@Xorplus# commit
```

set protocols bfd profile receive-interval

The **set protocols bfd profile receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a profile.

The **delete protocols bfd profile receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd profile shutdown

The **set protocols bfd profile shutdown** command can be used to disable a BFD peer. When the peer is disabled an 'administrative down' message is sent to the remote peer for a profile.

The **delete protocols bfd profile shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile *<profile-name>* **shutdown**

Parameter

Parameter	Description
profile *<profile-name>*	Specifies the profile name. The value is a string.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd profile p2 shutdown
admin@Xorplus# commit
```

set protocols bfd profile transmit-interval

The **set protocols bfd profile transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a profile.

The **delete protocols bfd profile transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 transmit-interval 500
admin@Xorplus# commit
```

set protocols bgp bfd

The **set protocols bgp bfd** command enables BFD for BGP.
The **delete protocols bgp bfd** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IP address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** can be used to modify parameters for a BFD session.

Example
• Enable BFD for BGP.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 bfd
admin@XorPlus# commit
```

set protocols ospf6 interface bfd

Run the command **set protocols ospf6 interface bfd** to enable BFD for OSPFv3 on the L3 interface.

Run the command **delete protocols ospf6 interface bfd** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols ospf6 interface <*interface-name***> bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** can be used to modify parameters for BFD session.

Example

- Enable BFD for OSPFv3 on the VLAN interface.

```
admin@XorPlus# set protocols ospf6 interface vlan200
admin@Xorplus# commit
```

set protocols ospf interface bfd

Run the command **set protocols ospf interface bfd** to enable BFD for OSPFv2 on the L3 interface.

Run the command **delete protocols ospf interface bfd** to remove this configuration.

Command Syntax

set protocols ospf interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols ospf interface <*interface-name***> bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** name can be used to modify parameters for BFD session.

Example

- Enable BFD for OSPFv2 on the VLAN interface.

```
admin@XorPlus# set protocols ospf interface vlan200 bfd
admin@Xorplus# commit
```

set protocols pim interface bfd

Run the command **set protocols pim interface bfd** to enables BFD for PIM on the L3 interface.

Run the command **delete protocols pim interface bfd** to remove this configuration.

Command Syntax

set protocols pim interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols pim interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*vlan-interface*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** name can be used to modify parameters for BFD session.

Example

- Enable BFD for PIM on the VLAN interface.

```
admin@XorPlus# set protocols pim interface vlan200 bfd
admin@Xorplus# commit
```

Policy-Based Routing (PBR) Commands

- set routing pbr map sequence match destination-ipv4
- set routing pbr map sequence match source-ipv4
- set routing pbr map sequence match destination-port
- set routing pbr map sequence match source-port
- set routing pbr map sequence match destination-ipv6
- set routing pbr map sequence match source-ipv6
- set routing pbr map sequence action nexthop
- set routing pbr map sequence action dscp
- set routing pbr map sequence action nexthop-group
- set routing nexthop-group nexthop-vrf nexthop
- set routing pbr map vlan-interface
- run show pbr map
- run clear pbr map

set routing pbr map sequence match destination-ipv4

The **set routing pbr map sequence match destination-ipv4** command configures a match rule based on the destination IPv4 address for PBR traffic classification.

The **delete routing pbr map sequence match destination-ipv4** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-ipv4** <*ipv4-address/*prefix-length>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-ipv4**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-ipv4 <*ipv4-address/prefix-length*>	Specifies destination IPv4 address, it should be an IPv4 subnet in the format of IPv4-address/prefix-length. For example, 10.1.1.0/24, 192.168.10.10/32.

Example

- Configure a match rule based on the destination IPv4 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-ipv4 10.1.1.0/24
admin@PICOS# commit
```

set routing pbr map sequence match source-ipv4

The **set routing pbr map sequence match source-ipv4** command configures a match rule based on the source IPv4 address for PBR traffic classification.

The **delete routing pbr map sequence match source-ipv4** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv4** <*ipv4-address/prefix-length*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match source-ipv4**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-ipv4 <*ipv4-address/prefix-length*>	Specifies source IPv4 address, it should be an IPv4 subnet in the format of IPv4-address/prefix-length. For example, 10.1.1.0/24.

Example

- Configure a match rule based on the source IPv4 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-ipv4 10.1.1.0/24
admin@PICOS# commit
```

set routing pbr map sequence match destination-port

The **set routing pbr map sequence match destination-port** command configures a match rule based on the destination port for PBR traffic classification.

The **delete routing pbr map sequence match destination-port** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-port** <*destination-port*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-port**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-port <*destination-port*>	Specifies the destination port number. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match rule based on the destination port for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-port 7000
admin@PICOS# commit
```

set routing pbr map sequence match source-port

The **set routing pbr map sequence match source-port** command configures a match rule based on the source port for PBR traffic classification.

The **delete routing pbr map sequence match source-port** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-port** <*source-port*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match source-port**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-port <*source-port*>	Specifies the source port number. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match rule based on the source port for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-port 7035
admin@PICOS# commit
```

set routing pbr map sequence match destination-ipv6

The **set routing pbr map sequence match destination-ipv6** command configures a match rule based on the destination IPv6 address for PBR traffic classification.

The **delete routing pbr map sequence match destination-ipv6** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-ipv6** <*ipv6-address/prefix-length*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-ipv6**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-ipv6 <*ipv6-address/prefix-length*>	Specifies destination IPv6 address, it should be an IPv6 subnet in the format of IPv6-address/prefix-length. For example, 2001::0/32.

Example

- Configure a match rule based on the destination IPv6 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-ipv6 2001::0/64
admin@PICOS# commit
```

set routing pbr map sequence match source-ipv6

The **set routing pbr map sequence match source-ipv6** command configures a match rule based on the source IPv6 address for PBR traffic classification.

The **delete routing pbr map sequence match source-ipv6** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv6** <*ipv6-address/prefix-length*>

delete routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv6**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-ipv6 <*ipv6-address/prefix-length*>	Specifies source IPv6 address, it should be an IPv6 subnet in the format of IPv6-address/prefix-length. For example, 2001::0/32.

Example

- Configure a match rule based on the source IPv6 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-ipv6 2001:a100::0/64
admin@PICOS# commit
```

set routing pbr map sequence action nexthop

The **set routing pbr map sequence action nexthop** command configures an action to redirect packets to a next-hop IP address for policy-based routing. The next-hop address must be directly connected and reachable without supporting recursion.

The **delete routing pbr map sequence action nexthop** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action nexthop** <*ip-address*> [**nexthop-vrf** <*vrf-name*>]

delete routing pbr map <*map-name*> **sequence** <*sequence-number*> **match action nexthop** <*ip-address*> [**nexthop-vrf**]

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
nexthop <*ip-address*>	Specifies next-hop IP, it could be a specific IPv4/IPv6 address. For example, 192.168.1.10.
nexthop-vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the next-hop route. • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Configure an action to redirect packets to a next-hop IP address for policy-based routing.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 action nexthop 10.30.1.10
admin@PICOS# commit
```

set routing pbr map sequence action dscp

The **set routing pbr map sequence action dscp** command configures an action to modify the DSCP value in packets for policy-based routing.

The **delete routing pbr map sequence action dscp** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action dscp** <*dscp-value*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **action dscp**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
dscp <*dscp-value*>	Specifies a value to modify the DSCP value in packets. The value is an integer in the range of 0 to 63.

Example

- Configure an action to modify the DSCP value in packets for policy-based routing.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 action dscp 40
admin@PICOS# commit
```

set routing pbr map sequence action nexthop-group

The **set routing pbr map sequence action nexthop-group** command configures an action to redirect packets to a next-hop group IP addresses for policy-based routing. The next-hop group addresses must be directly connected and reachable without supporting recursion.

The **delete routing pbr map sequence action nexthop-group** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action nexthop-group** <*group-name*>

delete routing pbr map <*map-name*> **sequence** <*sequence-number*> **match action nexthop-group**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
nexthop-group <*group-name*>	Specifies next-hop group name. The value is a string defined in the command **set routing nexthop-group** <*group-name*> **nexthop-vrf** <*vrf-name*> **nexthop** <*ip address*>.

Example

- Configure an action to redirect packets to a next-hop group for policy-based routing.

```
admin@PICOS# set routing nexthop-group group1 nexthop-vrf default nexthop 10.30.1.10
admin@PICOS# set routing nexthop-group group1 nexthop-vrf default nexthop 10.30.2.20
admin@PICOS# set routing pbr map PBR_map1 sequence 100 action nexthop-group group1
admin@PICOS# commit
```

set routing nexthop-group nexthop-vrf nexthop

The **set routing nexthop-group nexthop-vrf nexthop** command configures next-hop group addresses to direct traffic to a set of next-hops that reside in a particular VRF for policy-based routing. The next-hop addresses must be directly connected and reachable without supporting recursion.

The **delete routing nexthop-group nexthop-vrf nexthop** command deletes the configuration.

Command Syntax

set routing nexthop-group <*group-name*> **nexthop-vrf** <*vrf-name*> **nexthop** <*ip-address*>

delete routing nexthop-group <*group-name*> **nexthop-vrf** <*vrf-name*> **nexthop**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
nexthop-group <*group-name*>	Specifies next-hop group name. The value is a string.
nexthop-vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the next-hop route. • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When “**default**” is specified, find the next hop routing information from the default VRF.
nexthop <*ip-address*>	Specifies next-hop IP, it could be a specific IPv4/IPv6 address. For example, 192.168.1.10.

Usage Guidelines

This command is used to set up advanced routing where you need to direct traffic to a set of next-hops that reside in a particular VRF. This is often used in scenarios involving:

- **Multi-VRF configurations**: Where different services or customers have separate routing tables, but you want to manage next-hop forwarding for specific traffic.
- **Load balancing**: By defining a group of next-hops, you can balance traffic across multiple paths to improve network performance.
- **Traffic engineering**: In some cases, you might want to steer traffic through particular routers or paths within the network for optimization, redundancy, or policy enforcement.

When multiple next-hop IP addresses exist, the device performs redirection and forwarding of packets using load balancing. The device distributes the load based on the packet's 4-tuple: source/destination IP address and source/destination port, to select the next-hop.

Example

- Configure next-hop group addresses to direct traffic to a set of next-hops that reside in the default VRF for policy-based routing.

```
admin@PICOS# set routing nexthop-group group1 nexthop-vrf default nexthop 10.30.1.10
admin@PICOS# set routing nexthop-group group1 nexthop-vrf default nexthop 10.30.2.20
```

```
admin@PICOS# commit
```

set routing pbr map vlan-interface

The **set routing pbr map vlan-interface** command applies the PBR policy to the VLAN interface where the traffic is coming in.

The **delete routing pbr map vlan-interface** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **vlan-interface** <*vlan-interface*>

delete routing pbr map <*map-name*> **vlan-interface**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
vlan-interface <*vlan-interface*>	Specifies the VLAN interface name. The value is a string.

Example

- Apply the PBR policy on a VLAN interface.

```
admin@PICOS# set routing pbr map PBR_map1 vlan-interface vlan100
admin@PICOS# commit
```

run show pbr map

The **run show pbr map** command shows the configuration information of policy-based routing.

Command Syntax

run show pbr map [*<map-name>*]

Parameter

Parameter	Description
<map-name>	Optional. Specifies the map name of a PBR policy. The value is a string.

Example

- View the configuration information of policy-based routing.

```
admin@PICOS# run show pbr map
pbr-map        l3-interface
-----------    -------------
map1           vlan20

admin@PICOS# run show pbr map map1
Sequence: 1
    match-condition:
        destination-ipv4      1.1.1.0/24
    action:
        nexthop:20.0.0.1 nexthop-vrf:
    statistics:
        vlan2: 0 pkts

```

run clear pbr map

The **run show pbr map** command clears the statistics information of a PBR map.

> **NOTE:**
>
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run show pbr map <**all** | <*map-name*> [**sequence** <*sequence-number*>]>

Parameter

Parameter	Description
all | <*map-name*>	Specifies the map name of a PBR policy. The value is a string. When **all** is specified, clear the statistics information of all PBR maps.
sequence <*sequence-number*>	Optional. Specifies sequence number. The value is an integer that ranges from 1 to 700.

Example

- Clear the statistics information of a PBR map.

```
admin@PICOS# run clear pbr map map1
Pbr map statistics cleared.

admin@PICOS# run clear pbr map all
Pbr map statistics cleared.
```

IPv4 Source Guard (IPSG for IPv4) Commands

- set ip-source-guard binding ip
- set ip-source-guard enable
- set ip-source-guard verify
- set ip-source-guard traceoptions enable
- run show ip-source-guard binding

set ip-source-guard binding ip

The **set ip-source-guard binding ip** command configures a static IP source guard binding entry.

The **delete ip-source-guard binding ip** command deletes the configuration.

Command Syntax

set ip-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

delete ip-source-guard binding ip<*ip_address*> [**mac** <*mac-address*> **interface**<*interface-name*>**vlan** <*vlan-id*>]

Parameter

Parameter	Description
ip <*ip_address*>	Specifies a source IPv4 address for the static binding entry. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.
mac <*mac-address*>	Specifies a source MAC address for the static binding entry. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers, and cannot be all 0s, all Fs (a broadcast address), or a multicast address.
interface <*interface-name*>	Specifies ingress interface name for the static binding entry. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In IP Source Guard, static binding entries involve manually associating IP addresses with specific interfaces on a network device. IP Source Guard allows only traffic with matching source IP addresses and source MAC addresses to pass through the specified interface, thereby enhancing network security by preventing IP address spoofing attacks.

NOTE:

In the following example, a static IP source guard binding entry is configured on the device. When attempting to delete this entry, an error occurs.

```
set ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10

admin@PICOS# delete ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10
Deleting:
  10
OK
```

```
admin@PICOS# commit
IPSG: vlan is required for ip 110.100.10.2, mac 00:00:00:00:00:01, interface ge-1/1/1
Commit failed.

admin@PICOS# delete ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01
Deleting:
    00:00:00:00:00:01 {
                interface "ge-1/1/1" {
                    vlan 10
        }
    }
OK
admin@PICOS# commit
IPSG: mac is required for ip 110.100.10.2
Commit failed.
```

This is typically caused by the following two reasons:

- Due to the hierarchy structure design of PICOS CLI, when performing a deletion operation, the specified level and all its subordinate levels (i.e., the parameters and subsequent parameters in the command line) will be deleted, while the upper-level hierarchy (i.e., the parameters before the command line) will not be deleted.
- In the configuration of a static IP source guard binding entry, the command **set ip-source-guard binding ip** <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*> requires all four parameters: IP address, MAC address, interface name, and VLAN ID, to be configured.

For this type of deletion error, you can complete the deletion configuration by removing the first hierarchy level **ip-source-guard binding ip**.

```
admin@PICOS# delete ip-source-guard binding ip 110.100.10.2
Deleting:
    110.100.10.2 {
        mac 00:00:00:00:00:01 {
            interface "ge-1/1/1" {
                vlan 10
            }
        }
    }
OK

admin@PICOS# commit
Commit OK.
Save done.
```

Example

- Configure a static IP source guard binding entry manually.

```
admin@PICOS# set ip-source-guard binding ip 10.1.1.10 mac 22:22:22:11:11:11 interface ge-1/1/3 vlan 40
admin@PICOS# commit
```

set ip-source-guard enable

The **set ip-source-guard enable** command can be used to enable or disable IP source guard function based on ingress interface and VLAN of the packet.

The **delete ip-source-guard enable** command deletes the configuration.

Command Syntax

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**>

delete ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IP source guard static binding table, specifies the VLAN ID manually configured in IP source guard static binding table. • For IP source guard dynamic binding table, specifies the VLAN ID enabled DHCP snooping.
enable <**true	false**>	Enable or disable IP source guard function. The value could be **true** or **false**. • **true**: Enable IP source guard function. • **false**: Disable IP source guard function. By default, IP source guard function is disabled.

Usage Guidelines

IP source guard should be enabled based on specific interfaces and VLANs. When IP source guard is enabled based on a specific interface and VLAN, all packets from that interface and VLAN will be dropped except those that match entries in the IP source guard binding table.

Packets received from interfaces or VLANs that do not have IP source guard enabled will not be checked by the IP source guard module and will be processed as normal.

Example

- Enable IP source guard on interface ge-1/1/3 and VLAN 20.

```
admin@PICOS# set ip-source-guard interface ge-1/1/3 vlan 20 enable true
admin@PICOS# commit
```

set ip-source-guard verify

The **set ip-source-guard verify** command configures IP source guard filtering item based on specific interface and VLAN.

The **delete ip-source-guard verify** command deletes the configuration.

Command Syntax

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify <ip | ip+mac>**

delete ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IP source guard static binding table, specifies the VLAN ID manually configured in IP source guard static binding table. • For IP source guard dynamic binding table, specifies the VLAN ID enabled DHCP snooping.
verify <ip | ip+mac>	Specifies the filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**. • When "**ip**" is specified, enables IP Source Guard with *interface* + *VLAN* + *Source IP* filtering. • When "**ip+mac**" is specified, enables IP Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering. The default value is **ip**, IP Source Guard filtering item is interface + VLAN + Source IP.

Example

- Configure IP source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ip-source-guard interface te-1/1/3 vlan 20 verify ip+mac
admin@PICOS# commit
```

set ip-source-guard traceoptions enable

The **set ip-source-guard traceoptions enable** command can be used to enable or disable debugging for tracing IP source guard operations.

The **delete ip-source-guard traceoptions enable** command deletes the configuration.

Command Syntax

set ip-source-guard traceoptions enable <**true** | **false**>

delete ip-source-guard traceoptions enable

Parameter

Parameter	Description
disable <**true** | **false**>	Enable or disable debugging for tracing IP source guard operations. The value could be **true** or **false**. • **true**: Disable debugging for tracing IP source guard operations. • **false**: Enable debugging for tracing IP source guard operations. By default, debugging for tracing IP source guard operations is disabled.

Example

- Enable debugging for tracing IP source guard operations.

```
admin@PICOS# set ip-source-guard traceoptions enable true
admin@PICOS# commit
```

run show ip-source-guard binding

The **run show ip-source-guard binding** command shows the IP source guard binding entries.

Command Syntax

run show ip-source-guard binding [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled IP source guard. The value could be a physical port.

Example

- View the IP source guard binding entries.

```
admin@PICOS# run show ip-source-guard binding
Total ipsg host count:     5
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------
22:22:22:22:22:22   1.1.1.1          ge-1/1/3        20        static        ip                  effective
33:33:33:33:33:33   1.1.1.1          te-1/1/3        20        static        ip                  ineffective
22:22:22:11:11:11   10.1.1.10        ge-1/1/3        4094      static        ip+mac              ineffective
22:22:22:11:11:20   20.1.1.10        ge-1/1/3        1         dhcp-snooping ip+mac              ineffective
22:22:22:22:22:22   20.20.20.22      ge-1/1/3        6         static        ip+mac              ineffective
```

In the show result,

- The parameter “**Type**” indicates the type of the entry, the value could be **static** or **dhcp-snooping**:
  - Ø **static**: indicates that the entry is manually configured.
  - Ø **dhcp-snooping**: indicates that the entry is originated from the DHCP snooping binding table.
- The parameter “**Filter-type**” indicates the IP source guard filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**,
  - Ø **ip**: enables IP Source Guard with *interface* + *VLAN* + *Source IP* filtering.
  - Ø **ip+mac**: enables IP Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering.
- The parameter “**Status**” indicates whether the IP source guard binding entry is effective or not. After configuring the IP source guard binding entry, it needs to be deployed to the hardware by the system. If the entry is successfully deployed to the hardware, the "**Status**" will be shown as **effective**; however, if the deployment fails, it will be displayed as **ineffective**. Typically, the reason for deployment failure is due to the user configuring too many ACL rules, leading to insufficient hardware resources.

IPv6 Source Guard (IPSG for IPv6) Commands

- set ipv6-source-guard binding ip
- set ipv6-source-guard enable
- set ipv6-source-guard verify
- set ipv6-source-guard traceoptions enable
- run show ipv6-source-guard binding

set ipv6-source-guard binding ip

The **set ipv6-source-guard binding ip** command configures a static IPv6 source guard binding entry.

The **delete ipv6-source-guard binding ip** command deletes the configuration.

Command Syntax

set ipv6-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

delete ipv6-source-guard binding ip<*ip_address*> [**mac** <*mac-address*> **interface**<*interface-name*>**vlan** <*vlan-id*>]

Parameter

Parameter	Description
ip <*ip_address*>	Specifies a source IPv6 address for the static binding entry. The IPv6 address should be an unicast address.
mac <*mac-address*>	Specifies a source MAC address for the static binding entry. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers, and cannot be all 0s, all Fs (a broadcast address), or a multicast address.
interface <*interface-name*>	Specifies ingress interface name for the static binding entry. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In IPv6 Source Guard, static binding entries involve manually associating IP addresses with specific interfaces on a network device. IPv6 Source Guard allows only traffic with matching source IP addresses and source MAC addresses to pass through the specified interface, thereby enhancing network security by preventing IP address spoofing attacks.

NOTE:

In the following example, a static IPv6 source guard binding entry is configured on the device. When attempting to delete this entry, an error occurs.

```
set ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10

admin@PICOS# delete ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10
Deleting:
  10
OK
admin@PICOS# commit
```

```
IPSG6: vlan is required for ip 100::6, mac 00:00:00:00:00:01, interface ge-1/1/1
Commit failed.

admin@PICOS# delete ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01
Deleting:
    00:00:00:00:00:01 {
                  interface "ge-1/1/1" {
                      vlan 10
        }
    }
OK
admin@PICOS# commit
IPSG6: mac is required for ip 100::6
Commit failed.
```

This is typically caused by the following two reasons:

- Due to the hierarchy structure design of PICOS CLI, when performing a deletion operation, the specified level and all its subordinate levels (i.e., the parameters and subsequent parameters in the command line) will be deleted, while the upper-level hierarchy (i.e., the parameters before the command line) will not be deleted.
- In the configuration of a static IPv6 source guard binding entry, the command **set ipv6-source-guard binding ip** <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*> requires all four parameters: IP address, MAC address, interface name, and VLAN ID, to be configured.

For this type of deletion error, you can complete the deletion configuration by removing the first hierarchy level **ipv6-source-guard binding ip**.

```
admin@PICOS# delete ipv6-source-guard binding ip 100::6
Deleting:
    100::6 {
        mac 00:00:00:00:00:01 {
            interface "ge-1/1/1" {
                vlan 10
            }
        }
    }
OK

admin@PICOS# commit
Commit OK.
Save done.
```

Example

- Configure a static IPv6 source guard binding entry manually.

```
admin@PICOS# set ipv6-source-guard binding ip 100::6 mac 22:22:22:11:11:11 interface ge-1/1/3 vlan 40
admin@PICOS# commit
```

set ipv6-source-guard enable

The **set ipv6-source-guard enable** command can be used to enable or disable IPv6 source guard function based on ingress interface and VLAN of the packet.

The **delete ipv6-source-guard enable** command deletes the configuration.

Command Syntax

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**>

delete ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IPv6 source guard static binding table, specifies the VLAN ID manually configured in IPv6 source guard static binding table. • For IPv6 source guard dynamic binding table, specifies the VLAN ID enabled DHCPv6 snooping.
enable <**true	false**>	Enable or disable IPv6 source guard function. The value could be **true** or **false**. • **true**: Enable IPv6 source guard function. • **false**: Disable IPv6 source guard function. By default, IPv6 source guard function is disabled.

Usage Guidelines

IPv6 source guard should be enabled based on specific interfaces and VLANs. When IPv6 source guard is enabled based on a specific interface and VLAN, all packets from that interface and VLAN will be dropped except those that match entries in the IPv6 source guard binding table.

Packets received from interfaces or VLANs that do not have IPv6 source guard enabled will not be checked by the IPv6 source guard module and will be processed as normal.

Example

- Enable IPv6 source guard on interface ge-1/1/3 and VLAN 20.

```
admin@PICOS# set ipv6-source-guard interface ge-1/1/3 vlan 20 enable true
admin@PICOS# commit
```

set ipv6-source-guard verify

The **set ipv6-source-guard verify** command configures IPv6 source guard filtering item based on specific interface and VLAN.

The **delete ipv6-source-guard verify** command deletes the configuration.

Command Syntax

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify <ip | ip+mac>**

delete ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IPv6 source guard static binding table, specifies the VLAN ID manually configured in IPv6 source guard static binding table. • For IPv6 source guard dynamic binding table, specifies the VLAN ID enabled DHCPv6 snooping.
verify <ip | ip+mac>	Specifies the filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**. • When "**ip**" is specified, enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* filtering. • When "**ip+mac**" is specified, enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering. The default value is **ip**, IPv6 Source Guard filtering item is interface + VLAN + Source IP.

Example

- Configure IPv6 source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ipv6-source-guard interface te-1/1/3 vlan 20 verify ip+mac
admin@PICOS# commit
```

set ipv6-source-guard traceoptions enable

The **set ipv6-source-guard traceoptions enable** command can be used to enable or disable debugging for tracing IPv6 source guard operations.

The **delete ipv6-source-guard traceoptions enable** command deletes the configuration.

Command Syntax

set ipv6-source-guard traceoptions enable <**true** | **false**>

delete ipv6-source-guard traceoptions enable

Parameter

Parameter	Description
disable <**true** | **false**>	Enable or disable debugging for tracing IPv6 source guard operations. The value could be **true** or **false**. • **true**: Disable debugging for tracing IPv6 source guard operations. • **false**: Enable debugging for tracing IPv6 source guard operations. By default, debugging for tracing IPv6 source guard operations is disabled.

Example

- Enable debugging for tracing IPv6 source guard operations.

```
admin@PICOS# set ipv6-source-guard traceoptions enable true
admin@PICOS# commit
```

run show ipv6-source-guard binding

The **run show ipv6-source-guard binding** command shows the IPv6 source guard binding entries.

Command Syntax

run show ipv6-source-guard binding [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled IPv6 source guard. The value could be a physical port.

Example

- View the IPv6 source guard binding entries.

```
admin@PICOS# run show ipv6-source-guard binding
Total ipsg6 host count:     5
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------
22:22:22:22:22:22   2006::6           ge-1/1/3        20        static        ip                 effective
33:33:33:33:33:33   2007::7           te-1/1/3        20        static        ip                 ineffective
22:22:22:11:11:20   100::10           ge-1/1/3        1         dhcp6-snooping ip+mac             ineffective
22:22:22:22:22:22   2048::11          ge-1/1/3        6         static        ip+mac              ineffective
```

In the show result,

- The parameter “**Type**” indicates the type of the entry, the value could be **static** or **dhcp6-snooping**:
  - Ø **static**: indicates that the entry is manually configured.
  - Ø **dhcp6-snooping**: indicates that the entry is originated from the DHCPv6 snooping binding table.
- The parameter “**Filter-type**” indicates the IPv6 source guard filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**,
  - Ø **ip**: enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* filtering.
  - Ø **ip+mac**: enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering.
- The parameter “**Status**” indicates whether the IPv6 source guard binding entry is effective or not. After configuring the IPv6 source guard binding entry, it needs to be deployed to the hardware by the system. If the entry is successfully deployed to the hardware, the "**Status**" will be shown as **effective**; however, if the deployment fails, it will be displayed as **ineffective**. Typically, the reason for deployment failure is due to the user configuring too many ACL rules, leading to insufficient hardware resources.

ND Inspection Commands

- set protocols neighbour inspection vlan disable
- set protocols neighbour inspection validate source-mac
- set protocols neighbour inspection trust-port
- run show nd inspection dhcp6-snooping binding

set protocols neighbour inspection vlan disable

The **set protocols neighbour inspection vlan disable** command is used to enable or disable ND inspection function on a specific VLAN.

The **delete protocols neighbour inspection vlan disable** command deletes the configuration.

Command Syntax

set protocols neighbour inspection vlan <*vlan-id*> **disable** <**true | false**>

delete protocols neighbour inspection vlan <*vlan-id*> **disable**

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
disable <**true	false**>	Enable or disable ND inspection function on a specific VLAN. The value could be `true` or `false`. **true**: Disable ND inspection function. **false**: Enable ND inspection function. By default, ND inspection is disabled.

Usage Guidelines

The feature will check the arriving ND message source IPv6 address, and source MAC address against the NS/NA/RS/RA message with DHCPv6 snooping binding table.

- If the source IPv6 address, and source MAC address are the same, the device forwards the message.
- If the source IPv6 address, and source MAC address are not the same, the device considers the message is illegal and discards.

Example

- Enable ND inspection function on VLAN 1.

```
admin@PICOS# set protocols neighbour inspection vlan 1 disable false
admin@PICOS# commit
```

set protocols neighbour inspection validate source-mac

The **set protocols neighbour inspection validate source-mac** command can be used to enable ND inspection source MAC validation.

The **delete protocols neighbour inspection validate source-mac** command deletes the configuration.

Command Syntax

set protocols neighbour inspection validate source-mac

delete protocols neighbour inspection validate source-mac

Parameters

None.

Usage Guidelines

This feature verifies if the source MAC address matches the link-layer address of the received ND message.

- If the link-layer address and the MAC address are the same, the device forwards the message.
- If the link-layer address and the MAC address are not the same, the device considers the message is illegal and discarded.

Example

- Enable source MAC address check.

```
admin@PICOS# set protocols neighbour inspection validate source-mac
admin@PICOS# commit
```

set protocols neighbour inspection trust-port

The **set protocols neighbour inspection trust-port** command can be used to configure ND inspection trust port.

The **delete protocols neighbour inspection trust-port** command deletes the configuration.

Command Syntax

set protocols neighbour inspection trust-port *<port>*

delete protocols neighbour inspection trust-port *<port>*

Parameters

Parameter	Description
trust-port *<port>*	Specifies the trust port. The value could be a physical port or LAG port. The value is like ge-1/1/1, te-1/1/3, ae1, etc. **NOTE:** The device does not configure trust ports by default.

Usage Guidelines

This feature specifies the trust port, after specified, the device does not check ND message on that port and forwards the message.

Example

- Configure a ND inspection trust-port ge-1/1/1.

```
admin@PICOS# set protocols neighbour inspection trust-port ge-1/1/1
admin@PICOS# commit
```

run show nd inspection dhcp6-snooping binding

The **run show nd inspection dhcp6-snooping binding** command shows DHCPv6 snooping dynamic binding table entries used by ND inspection.

NOTEs:

Ensure that DHCPv6 snooping has formed complete table before using the following command.

Command Syntax

run show nd inspection dhcp6-snooping binding

Parameters

None.

Example

- View DHCPv6 snooping dynamic binding table entries used by ND inspection.

```
admin@PICOS# run show nd inspection dhcp6-snooping binding
Valid Dhcp6 Snooping host count:     2
VLAN ID               IPv6 Address              MAC Address
------------------------------------------------------------
20                       2001::1             22:22:22: 22:22:22
20                       2001::2             44:44:44: 44:44:44
```

ND Snooping Commands

- set protocols neighbour snooping vlan enable
- set protocols neighbour snooping trust-port
- set neighbour snooping max-user-number
- set protocols neighbour snooping static-prefix vlan
- run show neighbor snooping
- run show neighbor snooping prefix
- run show neighbor snooping binding
- run clear neighbor snooping prefix
- run clear neighbor snooping binding

set protocols neighbour snooping vlan enable

The **set protocols neighbour snooping vlan enable** command is used to enable or disable ND snooping protocol on a VLAN.

The **delete protocols neighbour snooping vlan enable** command deletes the configuration.

Command Syntax

set protocols neighbour snooping vlan <*vlan-id*> **enable** <**true** | **false**>

delete protocols neighbour snooping vlan <*vlan-id*> **enable**

Parameters

Parameter	Description
vlan < *vlan-id* >	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true | false**>	Enable or disable neighbour discovery snooping protocol on a specific VLAN. The value could be `true` or `false`. • **true**: Enable ND snooping protocol. • **false**: Disable ND snooping protocol. By default, ND snooping is disabled.

Example

- Enable neighbour discovery snooping protocol on VLAN 10.

```
admin@PICOS# set protocols neighbour snooping vlan 10 enable true
admin@PICOS# commit
```

set protocols neighbour snooping trust-port

The **set protocols neighbour snooping trust-port** command is used to configure a port as the trust port.

The **delete protocols neighbour snooping trust-port** command deletes the configuration.

Command Syntax

set protocols neighbour snooping trust-port <*port*>

delete protocols neighbour snooping trust-port [<*port*>]

Parameters

Parameter	Description
trust-port <*port*>	Specifies the port as a trust-port. The value could be a physical port or LAG port. The value is like ge-1/1/1, te-1/1/3, ae1, etc. By default, all ports of the device are untrusted.

Example

- Configure ND snooping trust-port.

```
admin@PICOS# set protocols neighbour snooping trust-port ge-1/1/1
admin@PICOS# commit
```

set neighbour snooping max-user-number

The **set protocols neighbour snooping max-user-number** command is used to configure the maximum number of ND snooping dynamic binding table entries a device allowed to learn.

The **delete protocols neighbour snooping max-user-number** command restores the configuration to the default value.

Command Syntax

set protocols neighbour snooping max-user-number <*max-user-num*>

delete protocols neighbour snooping max-user-number

Parameters

Parameter	Description
max-user-number <*max-user-num*>	Specifies the maximum number of ND snooping dynamic binding table entries that the device is allowed to learn. The value is an integer that ranges from 1 to 9216. The default value is 9216.

Usage Guidelines

Mass NS messages will cause the ND snooping dynamic binding table resources to be exhausted, and user can configure the maximum number of ND snooping dynamic binding table entries that the device is allowed to learn. If the number of entries reaches the maximum number, new entries related to the device cannot to be added.

Example

- Configure maximum number dynamic binding table entries for a device.

```
admin@PICOS# set protocols neighbour snooping max-user-number 1000
admin@PICOS# commit
```

set protocols neighbour snooping static-prefix vlan

The **set protocols neighbour snooping static-prefix vlan** command is used to configure static prefix management table entries.

The **delete protocols neighbour snooping static-prefix vlan** command deletes the configuration.

Command Syntax

set protocols neighbour snooping static-prefix < *IPv6Net* **> vlan <***vlan-id***>**

delete protocols neighbour snooping static-prefix < *IPv6Net* **> vlan <***vlan-id***>**

Parameters

Parameters	Description
static-prefix < *IPv6Net***>**	Specifies the IPv6 prefix, e.g. fa00::0/64.
vlan <*vlan-id***>**	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

A device can generate a prefix management table by listening to RA messages received from the ND snooping trust port. If the device does not send RA messages, the prefix management table entries cannot automatically generate, thus user can configure the corresponding ND snooping dynamic binding table entries.

Example

- Configure a static prefix management table entry, the IPv6 address prefix of the table entry is fa00::0/64.

```
admin@PICOS# set protocols neighbour snooping static-prefix fa00::0/64 vlan 10
admin@PICOS# commit
```

run show neighbor snooping

The **run show neighbor snooping** command is used to view configuration information of the current device.

Command Syntax

run show neighbor snooping

Parameter

None.

Example

- View ND snooping configuration of the device.

```
admin@PICOS# run show neighbor snooping
ND Snooping enabled vlans: 10, 20, 30, 40, 50, 60
ND Snooping trust-ports: ge-1/1/1, ae2
ND Snooping max-user-number: 9216
```

run show neighbor snooping prefix

The **run show neighbor snooping prefix** command is used to view neighbour discovery snooping prefix management table.

Command Syntax

run show neighbor snooping prefix [**static | dynamic**]

Parameter

Parameters	Description
[**static | dynamic**]	Optional. Indicates to show the ND snooping prefix management table configured statically or learned dynamically. If not specified, the device shows all ND snooping prefix management table entries.

Example

- View all the ND snooping prefix management table.

```
admin@PICOS# run show neighbor snooping prefix
Total Snooping table prefix count:    2
Total Snooping table dynamic count:  1
Total Snooping table static count:     1
Prefix          Length   Port    VLAN ID   Valid-Time   Prefix-Type
-----------------------------------------------------------------
FC00:1::       64       ge-1/1/2    10        100/120      Dynamic
2001:1::        64       ge-1/1/1    10        35/120       Static
```

- View statically configured ND snooping prefix management table.

```
admin@PICOS# run show neighbor snooping prefix static
Total Snooping table static count: 1
Prefix         Length   Port      VLAN ID   Valid-Time    Prefix-Type
-----------------------------------------------------------------------
2001:1::        64     ge-2/1/1     10         35/120       Static
```

- View dynamically learned ND snooping prefix management table.

```
admin@PICOS# run show neighbor snooping prefix dynamic
Total Snooping table dynamic count:     1
Prefix         Length   Port    VLAN ID   Valid-Time    Prefix-Type
-----------------------------------------------------------------------
FC00:1::        64     ge-1/1/2   10        100/120      Dynamic
```

run show neighbor snooping binding

The **run show neighbor snooping binding** command is used to view ND snooping dynamic management table.

Command Syntax

run show neighbor snooping binding

Parameter

None.

Example

- View ND snooping dynamic management table.

```
admin@PICOS# run show neighbor snooping binding
Total ND Snooping binding count: 2
MAC Address      IPv6 Address        Port    VLAN ID   Status    Lease(sec)
------------------------------------------------------------------------------
22:22:22: 22:22:21   FC00:1::E58C:A2E7  ge-1/1/1   10      Valid      99/120
44:44:44: 44:22:21   FC00:1::E58C:A2E6  ge-1/1/2   20      Valid      89/120
```

run clear neighbor snooping prefix

The **run clear neighbor snooping prefix** command is used to clear dynamically learned ND snooping prefix management table.

Command Syntax

run clear neighbor snooping prefix

Parameter

None.

Example

- Clear ND snooping prefix management table.

```
admin@PICOS# run clear neighbor snooping prefix
```

run clear neighbor snooping binding

The **run clear neighbor snooping binding** command is used to clear ND snooping dynamic management table.

Command Syntax

run clear neighbor snooping binding

Parameter

None.

Example

- Clear ND snooping dynamic management table.

```
admin@PICOS# run clear neighbor snooping binding
```

IS-IS commands

- set protocols isis area-tag network-entity
- set protocols isis area-tag is-type
- set protocols isis area-tag interface
- set protocols isis area-tag hostname-dynamic
- set protocols isis area-tag area-password authentication-type
- set protocols isis area-tag area-password authentication-key
- set protocols isis area-tag area-password authenticate-snp
- set protocols isis area-tag domain-password authentication-type
- set protocols isis area-tag domain-password authentication-key
- set protocols isis area-tag domain-password authenticate-snp
- set protocols isis area-tag attached-bit receive-ignore
- set protocols isis area-tag attached-bit send
- set protocols isis area-tag log-adjacency-changes
- set protocols isis area-tag metric-style
- set protocols isis area-tag set-overload-bit
- set protocols isis area-tag purge-originator
- set protocols isis area-tag lsp-mtu
- set protocols isis area-tag lsp-timers gen-interval
- set protocols isis area-tag lsp-timers refresh-interval
- set protocols isis area-tag lsp-timers max-lifetime
- set protocols isis area-tag spf-interval
- set protocols isis area-tag spf-delay-ietf init-delay
- set protocols isis area-tag spf-delay-ietf short-delay
- set protocols isis area-tag spf-delay-ietf long-delay
- set protocols isis area-tag spf-delay-ietf holddown
- set protocols isis area-tag spf-delay-ietf time-to-learn
- set protocols isis area-tag default-information originate
- set protocols isis area-tag default-information originate metric
- set protocols isis area-tag default-information originate route-map
- set protocols isis area-tag topology ipv6-unicast
- set protocols isis area-tag interface circuit-type
- set protocols isis area-tag interface csnp-interval
- set protocols isis area-tag interface psnp-interval
- set protocols isis area-tag interface hello-padding
- set protocols isis area-tag interface hello-interval
- set protocols isis area-tag interface hello-multiplier
- set protocols isis area-tag interface metric
- set protocols isis area-tag interface network point-to-point
- set protocols isis area-tag interface passive
- set protocols isis area-tag interface password authentication-type
- set protocols isis area-tag interface password authentication-key
- set protocols isis area-tag interface priority
- set protocols isis area-tag interface three-way-handshake
- set protocols isis area-tag interface bfd
- set protocols isis area-tag interface topology ipv6-unicast
- set protocols isis area-tag redistribute

- set protocols isis traceoption events
- set protocols isis traceoption adj-packets
- set protocols isis traceoption route-events
- set protocols isis traceoption snp-packets
- run show isis summary
- run show isis interface
- run show isis database
- run show isis hostname
- run show isis neighbor
- run show isis route
- run show isis topology

set protocols isis area-tag network-entity

The **set protocols isis area-tag network-entity** command configures network entity title (NET) provided in ISO format. The NET defines the current IS-IS area address and the system ID of the device.

The **delete protocols isis area-tag network-entity** command deletes the configuration.

NOTEs:

- The area address is used to uniquely identify different areas within a routing domain. All switches within the same Level-1 area must have the same area address, while switches within Level-2 areas can have different area addresses.
- Throughout the entire domain and backbone area, it is required to maintain a unique system ID.
- Currently, the switch supports only one IS-IS routing instance per VRF.
- Since a maximum of 3 area addresses can be configured in an IS-IS process, only up to 3 NETs can be configured.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **network-entity** <*network-entity*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **network-entity** <*network-entity*>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
network-entity <*network-entity*>	Specifies the network entity title (NET) name.

Usage Guidelines

The NET consists of three parts:

- Area ID: The length of the Area ID can vary from 1 to 13 bytes.
- System ID: This part has a fixed length of 6 bytes.
- NSAP Selector (SEL): The last byte, different transport protocols correspond to different SELs. For IP, the SEL is always 00.

When configuring the NET parameter in IS-IS, ensure that these three components are properly defined according to your network requirements.

Example

- Define the NET as 32.0001.0040.0220.2030.00. The system ID is 0040.0220.2030 and the area ID is 32.0001.

```
admin@PICOS# set protocols isis area-tag instance1 network-entity 32.0001.0040.0220.2030.00
admin@PICOS# commit
```

set protocols isis area-tag is-type

The **set protocols isis area-tag is-type** command configures the level of the IS-IS switch.

The **delete protocols isis area-tag is-type** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **is-type**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
is-type <**level-1** | **level-1-2** | **level-2-only**>	Specifies the level of the IS-IS switch. The value could be **level-1**, **level-1-2** or **level-2-only**. The default value is **level-1-2**.

Example

- Configure the level of the IS-IS switch.

```
admin@PICOS# set protocols isis area-tag instance1 is-type level-1
admin@PICOS# commit
```

set protocols isis area-tag interface

The **set protocols isis area-tag interface** command enables IS-IS instance on a specific interface.

The **delete protocols isis area-tag interface** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> <**ipv4-routing | ipv6-routing**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> <**ipv4-routing | ipv6-routing**>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface. By default, IS-IS is disabled on the interface.
<**ipv4-routing	ipv6-routing**>	Specifies the IP routing type.

Example

- Enable IS-IS instance on a specific interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 ipv4-routing
admin@PICOS# commit
```

set protocols isis area-tag hostname-dynamic

The **set protocols isis area-tag hostname-dynamic** command enables support for dynamic hostname.

The **delete protocols isis area-tag hostname-dynamic** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **hostname-dynamic** <**enable** | **disable**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **hostname-dynamic**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**enable** | **disable**>	Enable or disable dynamic hostname. The value could be **enable** or **disable**. • **enable**: Enable dynamic hostname. • **disable**: Disable dynamic hostname. By default, dynamic hostname is enabled.

Example

- Enable support for dynamic hostname.

```
admin@PICOS# set protocols isis area-tag instance1 hostname-dynamic enable
admin@PICOS# commit
```

set protocols isis area-tag area-password authentication-type

The **set protocols isis area-tag area-password authentication-type** command configures authentication type for the IS-IS area. The command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password authentication-key** <*password*> can be used to configure the authentication key. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag area-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type to *md5*.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag area-password authentication-key

The **set protocols isis area-tag area-password authentication-key** command configures authentication key for the IS-IS area. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag area-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authentication-key** <*password*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag area-password authenticate-snp

The **set protocols isis area-tag area-password authenticate-snp** command configures the authentication method for SNP messages in the IS-IS area. By default, IS-IS does not encapsulate authentication information for the sent SNP messages, nor perform authentication checks on the received SNP messages. Users can use this command to change this behavior.

The **delete protocols isis area-tag area-password authenticate-snp** command deletes the configuration.

NOTE:

Before configuring authenticate-snp, the authentication-type and authentication-key should be configured first.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authenticate-snp** <**none**|**send-only**|**validate**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authenticate-snp**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
none	IS-IS neither encapsulates authentication information for the sent SNP messages nor performs authentication checks on the received SNP messages.
send-only	Specifies encapsulating authentication information for generated LSPs and SNPs; only verify received LSPs, and do not verify received SNPs.
validate	IS-IS encapsulates authentication information for the sent SNP messages and performs authentication checks on the received SNP messages.

Example

- Configure the system only to encapsulate authentication information for the sent SNP messages for the IS-IS area.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authenticate-snp send-only
admin@PICOS# commit
```

set protocols isis area-tag domain-password authentication-type

The **set protocols isis area-tag domain-password authentication-type** command configures authentication type for the IS-IS domain. The command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-key** <*password*> can be used to configure the authentication key. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag domain-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type to *md5*.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag domain-password authentication-key

The **set protocols isis area-tag domain-password authentication-key** command configures authentication key for the IS-IS domain. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag domain-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-key** <*password*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag domain-password authenticate-snp

The **set protocols isis area-tag domain-password authenticate-snp** command configures the authentication method for SNP messages for the IS-IS domain. By default, IS-IS does not encapsulate authentication information for the sent SNP messages, nor perform authentication checks on the received SNP messages. Users can use this command to change this behavior.

The **delete protocols isis area-tag domain-password authenticate-snp** command deletes the configuration.

NOTE:

Before configuring authenticate-snp, the authentication-type and authentication-key should be configured first.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authenticate-snp** <**send-only**|**validate**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authenticate-snp**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
send-only	Specifies encapsulating authentication information for generated LSPs and SNPs; only verify received LSPs, and do not verify received SNPs.
validate	IS-IS encapsulates authentication information for the sent SNP messages and performs authentication checks on the received SNP messages.

Example

- Configure the system only to encapsulate authentication information for the sent SNP messages for the IS-IS domain.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authenticate-snp send-only
admin@PICOS# commit
```

set protocols isis area-tag attached-bit receive-ignore

The **set protocols isis area-tag attached-bit receive-ignore** command can be configured to prevent Level-1 routers from generating default routes due to the ATT bit. After configuration, Level-1 routers will not generate default routes in the routing table due to the ATT bit.

The **delete protocols isis area-tag attached-bit receive-ignore** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit receive-ignore** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit receive-ignore**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
receive-ignore <**true** | **false**>	Specifies whether Level-1 routers generate default routes due to the ATT bit. The value could be **true** or **false**. • **true**: Level-1 routers don't generate default routes due to the ATT bit. • **false**: Level-1 routers generate default routes due to the ATT bit. The default value is **false**.

Usage Guidelines

The ATT bit is a field in IS-IS LSP (Link State Packet) messages used to indicate whether a Level-1 area is connected to other areas. Level-1-2 routers set this field in their generated Level-1 LSPs to inform Level-1 routers within the same area that they are connected to other areas, specifically to the Level-2 backbone area. When routers in a Level-1 area receive Level-1 LSPs with the ATT bit set from Level-1-2 routers, they create a default route pointing to the Level-1-2 router as the destination, allowing data to be routed to other areas.

To prevent Level-1 routers from generating default routes due to the ATT bit, this command can be configured. After configuration, Level-1 routers will not send default routes in the routing table due to the ATT bit.

Example

- Configure Level-1 routers not to generate default routes in the routing table due to the ATT bit.

```
admin@PICOS# set protocols isis area-tag instance1 attached-bit receive-ignore true
admin@PICOS# commit
```

set protocols isis area-tag attached-bit send

The **set protocols isis area-tag attached-bit send** command configures that whether the Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers.

The **delete protocols isis area-tag attached-bit send** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit send** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit send**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
send <**true** | **false**>	Specifies whether the Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers. The value could be **true** or **false**. • **true**: Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers. • **false**: Level-1-2 routers don't set ATT bit in the LSP sent to Level-1 routers. The default value is **true**.

Example

- Configure the Level-1-2 routers to set ATT bit in the LSP sent to Level-1 routers.

```
admin@PICOS# set protocols isis area-tag instance1 attached-bit send true
admin@PICOS# commit
```

set protocols isis area-tag log-adjacency-changes

The **set protocols isis area-tag log-adjacency-changes** command opens the log of neighbor status changes.

The **delete protocols isis area-tag log-adjacency-changes** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **log-adjacency-changes**

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **log-adjacency-changes**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

When IS-IS detects a change in neighbor relationships, record the change in the system log.

Example

- Open the log of neighbor status changes.

```
admin@PICOS# set protocols isis area-tag instance1 log-adjacency-changes
admin@PICOS# commit
```

set protocols isis area-tag metric-style

The **set protocols isis area-tag metric-style** command configures the metric behavior transmitted by this router and the received metric behavior that will be used for processing the SPF calculation by this router.

The **delete protocols isis area-tag metric-style** command deletes the configuration.

- If you need to modify the IS-IS route metric type, please configure the **metric-style** when setting up the basic IS-IS functions. Otherwise, changing the metric type during network operation will cause the IS-IS process to restart, which may lead to neighbor disconnections.
- When setting the IS-IS metric type, be cautious as the metric type settings on the connected devices at both ends will affect link reachability.
- If the **metric-style** is not ***wide***, the metric value for IS-IS interface must be less than 64.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **metric-style** <**narrow** | **transition** | **wide**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **metric-style**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
metric-style <**narrow** | **transition** | **wide**>	Specifies the old-style (ISO 10589) or new-style packet formats. The value could be **narrow**, **transition** or **wide**. • **narrow**: transmit only narrow IS-IS metrics and to only process received narrow metrics from other routers for this router's SPF calculation. • **transition**: transmit both narrow and wide metrics, and if both metrics are received, to process the narrow metrics for this router's SPF calculation. If only wide metrics are received, wide metrics will be used for this router's SPF calculation. • **wide**: transmit only wide IS-IS metrics, and to only process received wide metrics from other routers for this router's SPF calculation. The default value is **wide**.

Usage Guidelines

Configuring metric style determines which metric behavior received from other IS-IS routers will be processed for this router's SPF calculation, and which metric behavior will be transmitted to other IS-IS routers by this router. The metric style used by an IS-IS router can be either narrow or wide.

Example

- Configure to transmit only narrow IS-IS metrics.

```
admin@PICOS# set protocols isis area-tag instance1 metric-style narrow
admin@PICOS# commit
```

set protocols isis area-tag set-overload-bit

The **set protocols isis area-tag set-overload-bit** command configures the overload bit for non-pseudonode LSPs.

The **delete protocols isis area-tag set-overload-bit** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **set-overload-bit** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **set-overload-bit**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true** | **false**>	Specifies whether to configure the overload bit for non-pseudonode LSPs. The value could be **true** or **false**. • **true**: configure the overload bit for non-pseudonode LSPs. • **false**: not configure the overload bit for non-pseudonode LSPs. The default value is **false**.

Usage Guidelines

Although an LSP with the overload bit set will propagate throughout the network, it will not be used when calculating routes through an overloaded switch. That is to say, after setting the overload bit for a switch, other switches will not consider this switch when performing SPF calculations. However, direct routes to this switch will not be ignored.

Example

- Configure the overload bit for non-pseudonode LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 set-overload-bit true
admin@PICOS# commit
```

set protocols isis area-tag purge-originator

The **set protocols isis area-tag purge-originator** command is used to enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. Once this functionality is enabled, if dynamic hostname configuration is also set locally, the hostname TLV will be added in the PURGE messages as well.
The **delete protocols isis area-tag purge-originator** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **purge-originator** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **purge-originator**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true** | **false**>	Enable or disable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. The value could be **true** or **false**. • **true**: enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. • **false**: disable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. The default value is **false**.

Usage Guidelines

When the Remaining Lifetime field of an LSP message is 0, it indicates that the message has expired, and it is then referred to as a PURGE message. Typically, PURGE messages do not contain any information about the device that generated them, making it difficult to identify the source of the message when network issues occur.

To address this issue, the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **purge-originator** command can be used to add the POI (Purge-Originator-Identification) TLV in PURGE messages sent by IS-IS devices. Additionally, if dynamic hostname configuration is enabled locally, the hostname TLV will also be added to the PURGE messages, providing convenience for troubleshooting purposes.

Example

- Enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally.

```
admin@PICOS# set protocols isis area-tag instance1 purge-originator true
admin@PICOS# commit
```

set protocols isis area-tag lsp-mtu

The **set protocols isis area-tag lsp-mtu** command configures the maximum size of generated LSPs, in bytes.

The **delete protocols isis area-tag lsp-mtu** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-mtu** <*max-size*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-mtu**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
lsp-mtu <*max-size*>	Specifies the maximum size of generated LSPs. The value is an integer ranging from 128 to 4352 bytes. The default value is 1497 bytes.

Usage Guidelines

This command configures the size of the LSP (Link State Protocol) messages generated and received by the current IS-IS system.

NOTE:

Make sure that the length of the LSP is smaller than the MTU (Maximum Transmission Unit) of the IS-IS interface, otherwise, the LSP messages cannot be sent properly.

Example

- Configure the maximum size of generated LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-mtu 1024
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers gen-interval

The **set protocols isis area-tag lsp-timers gen-interval** command configures the minimum interval in seconds between regenerating same LSP.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers gen-interval** <*lsp-gen-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
gen-interval <*lsp-gen-interval*>	Specifies the minimum interval between regenerating same LSP. The value is an integer ranging from 2 to 65235 seconds. The default value is 900 seconds.

Usage Guidelines

When there are changes in local routing information, the device needs to generate new LSPs to announce these changes. When changes in local routing information occur frequently, immediately generating new LSPs consumes a large amount of system resources. To speed up network convergence without affecting system performance, you can adjust the interval between LSP generations using this command.

Example

- Configure the minimum interval in seconds between regenerating same LSP.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers gen-interval 500
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers refresh-interval

The **set protocols isis area-tag lsp-timers refresh-interval** command configures the refresh interval for LSPs.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.
- The LSP maximum lifetime must exceed the refresh interval by more than 300.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers refresh-interval** <*lsp-refresh-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
refresh-interval <*lsp-refresh-interval*>	Specifies the refresh interval for LSPs. The value is an integer ranging from 1 to 65235 seconds. The default value is 900 seconds.

Usage Guidelines

The flooding of LSPs (Link State Packets) requires periodic refreshing because when a device generates its system LSP, it includes the maximum valid time for the LSP. As other devices receive this LSP, its valid time decreases over time. If a device does not receive an updated LSP, once the valid time of the LSP reaches 0, it will be retained for an additional 60 seconds. If a new LSP is not received within this time, the LSP will be deleted.

By using command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers refresh-interval** <*lsp-refresh-interval*> to configure the refresh period for LSPs, it ensures that LSPs remain within their valid period and controls the convergence speed of the network.

Example

- Configure the refresh interval for LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers refresh-interval 1800
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers max-lifetime

The **set protocols isis area-tag lsp-timers max-lifetime** command configures the maximum valid time for the LSPs generated by IS-IS. Adjust the maximum valid time for LSPs to ensure the validity of old LSPs until updated LSPs are received.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.
- The LSP maximum lifetime must exceed the refresh interval by more than 300.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers max-lifetime** <*max-lsp-lifetime*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
max-lifetime <*max-lsp-lifetime*>	Specifies the maximum valid time for the LSPs generated by IS-IS. The value is an integer ranging from 350 to 65535 seconds. The default value is 1200 seconds.

Usage Guidelines

The maximum lifetime of a link-state packet determines how long a link state packet will be propagated around the network before it is considered unusable. When an LSP's age reaches the 0, the packet is no longer usable.

Example

- Configure the maximum valid time for the LSPs generated by IS-IS.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers max-lifetime 2000
admin@PICOS# commit
```

set protocols isis area-tag spf-interval

The **set protocols isis area-tag spf-interval** command configures the interval time for SPF (Shortest Path First) calculation.

The **delete protocols isis area-tag spf-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-interval** <*spf-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
spf-interval <*spf-interval*>	Specifies the interval time for SPF (Shortest Path First) calculation. The value is an integer ranging from 1 to 120 seconds. The default value is 1 seconds.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

Example

- Configure the interval time for SPF (Shortest Path First) calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-interval 60
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf init-delay

The **set protocols isis area-tag spf-delay-ietf init-delay** command configures the initial delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf init-delay** <*init-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
init-delay <*init-delay*>	Specifies the initial delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the initial delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf init-delay 50
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf short-delay

The **set protocols isis area-tag spf-delay-ietf short-delay** command configures the short delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf short-delay** <*short-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
short-delay <*short-delay*>	Specifies the short delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the short delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf short-delay 10
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf long-delay

The **set protocols isis area-tag spf-delay-ietf long-delay** command configures the long delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf long-delay** <*long-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
long-delay <*long-delay*>	Specifies the long delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the long delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf long-delay 500
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf holddown

The **set protocols isis area-tag spf-delay-ietf holddown** command configures the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf holddown** <*holddown*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
holddown <*holddown*>	Specifies the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Example

- Configure the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf holddown 120
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf time-to-learn

The **set protocols isis area-tag spf-delay-ietf time-to-learn** command configure the maximum duration typically needed to learn all the IGP events related to a single component failure (such as router failure or SRLG failure).

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf time-to-learn** <*time-to-learn*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
time-to-learn <*time-to-learn*>	Specifies the maximum duration typically needed to learn all the IGP events related to a single component failure. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

It's mostly dependent on failure detection time variation between all routers that are adjacent to the failure. Additionally, it may depend on the different IGP implementations/parameters across the network and their relation to the origination and flooding of link state advertisements.

Example

- Configure the maximum duration typically needed to learn all the IGP events related to a single component failure.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf time-to-learn 3600
admin@PICOS# commit
```

set protocols isis area-tag default-information originate

The **set protocols isis area-tag default-information originate** command generates a default route in IS-IS route. Adding **always** argument to the "default-infomation orginate" statement essentially skips the checking for a default route already being installed in the table.

The **delete protocols isis area-tag default-information originate** command deletes the configuration.

When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** configuration in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> [**always**]

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**><**level-1** | **level-2**> [**always**]

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.

Example

- Generate a default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 always
admin@PICOS# commit
```

set protocols isis area-tag default-information originate metric

The **set protocols isis area-tag default-information originate metric** command configures the metric for the default route in IS-IS route.

The **delete protocols isis area-tag default-information originate metric** command deletes the configuration.

When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** set in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **metric** <*metric*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **metric**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
metric <*metric*>	Specifies the metric for the generated default route. The value is an integer ranging from 0 to 16777215.

Example

- Configure the metric for the default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 metric 50
admin@PICOS# commit
```

set protocols isis area-tag default-information originate route-map

The **set protocols isis area-tag default-information originate route-map** command configures the route map for the default route in IS-IS route.

The **delete protocols isis area-tag default-information originate route-map** command deletes the configuration.

When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** set in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **route-map** <*route-map*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **route-map**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
route-map <*route-map*>	Specifies the route map name for the generated default route. The value is a string.

Example

- Configure the route map for the default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 route-map
map1
admin@PICOS# commit
```

set protocols isis area-tag topology ipv6-unicast

The **set protocols isis area-tag topology ipv6-unicast** command enables an IPv6 unicast topology for IS-IS.

The **delete protocols isis area-tag topology ipv6-unicast** command deletes the configuration.

To enable IPv6 unicast topology for IS-IS, the **metric-style** configuration should not be **narrow**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast** [**overload**]

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

- Enable an IPv6 unicast topology for IS-IS.

```
admin@PICOS# set protocols isis area-tag instance1 topology ipv6-unicast
admin@PICOS# commit
```

set protocols isis area-tag interface circuit-type

The **set protocols isis area-tag interface circuit-type** command configures circuit type for interface.

The **delete protocols isis area-tag interface circuit-type** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **circuit-type** <**level-1** | **level-1-2** | **level-2**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **circuit-type** <**level-1** | **level-1-2** | **level-2**>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
circuit-type <**level-1** | **level-1-2** | **level-2**>	Specifies the circuit type for interface. • **level-1**: Level-1 only adjacencies are formed. • **level-1-2**: Level-1-2 adjacencies are formed. • **level-2**: Level-2 only adjacencies are formed.

Example

- Configure circuit type for interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 circuit-type level-1
admin@PICOS# commit
```

set protocols isis area-tag interface csnp-interval

The **set protocols isis area-tag interface csnp-interval** command is used to specify the interval for sending CSNP messages on a broadcast network.

The **delete protocols isis area-tag interface csnp-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **csnp-interval** <*csnp-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **csnp-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
csnp-interval <*csnp-interval*>	Specifies the interval for sending CSNP messages. The value is an integer ranging from 1 to 600 seconds. The default value is 10 seconds.

Example

- Configure the interval for sending CSNP messages on a broadcast network.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 csnp-interval 50
admin@PICOS# commit
```

set protocols isis area-tag interface psnp-interval

The **set protocols isis area-tag interface psnp-interval** command configures the Partial Sequence Number Packets (PSNP) interval in seconds.

The **delete protocols isis area-tag interface psnp-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **psnp-interval** <*psnp-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **psnp-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
psnp-interval <*psnp-interval*>	Specifies the Partial Sequence Number Packets (PSNP) interval. The value is an integer ranging from 1 to 120 seconds. The default value is 2 seconds.

Example

- Configure the Partial Sequence Number Packets (PSNP) interval.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 psnp-interval 50
admin@PICOS# commit
```

set protocols isis area-tag interface hello-padding

The **set protocols isis area-tag interface hello-padding** command is used to configure IS-IS interfaces to send standard Hello messages with padding fields.

The **delete protocols isis area-tag interface hello-padding** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-padding** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-padding**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-padding <**enable** | **disable**>	Enable or disable IS-IS interfaces to send standard Hello messages with padding fields. The value could be **enable** or **disable**. • **enable**: Enables IS-IS interfaces to send standard Hello messages with padding fields. • **disable**: Disables IS-IS interfaces to send standard Hello messages with padding fields. By default, IS-IS interfaces send standard Hello messages with padding fields.

Example

- Configure IS-IS interfaces to send standard Hello messages with padding fields.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-padding enable
admin@PICOS# commit
```

set protocols isis area-tag interface hello-interval

The **set protocols isis area-tag interface hello-interval** command is used to specify the interval time for sending Hello messages on an IS-IS interface.

The **delete protocols isis area-tag interface hello-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-interval** <*hello-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-interval <*hello-interval*>	Specifies the interval for sending Hello messages. The value is an integer ranging from 1 to 600 seconds. The default value is 3 seconds.

Example

- Configure the interval time for sending Hello messages on an IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-interval 30
admin@PICOS# commit
```

set protocols isis area-tag interface hello-multiplier

The **set protocols isis area-tag interface hello-multiplier** command configures the multiplier for the interval time between Hello messages, in order to modify the neighbor hold time of IS-IS. The neighbor hold time is **hello-interval** x **hello-multiplier**.

The **delete protocols isis area-tag interface hello-multiplier** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-multiplier** <*integer*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-multiplier**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-multiplier <*integer*>	Specifies the neighbor hold time as a multiple of the interval time between Hello messages. The value is an integer ranging from 2 to 100. The default value is 10.

Example

- Configure the multiplier for the interval time between Hello messages.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-multiplier 30
admin@PICOS# commit
```

set protocols isis area-tag interface metric

The **set protocols isis area-tag interface metric** command configures default metric value for IS-IS interface.

The **delete protocols isis area-tag interface metric** command deletes the configuration.

If the **metric-style** is not ***wide***, the metric value for IS-IS interface must be less than 64.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **metric** <*metric*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **metric**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
metric <*metric*>	Specifies the default metric value for IS-IS interface. The value is an integer ranging from 0 to 16777215. The default value is 10.

Example

- Configure the default metric value for IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 metric 100
admin@PICOS# commit
```

set protocols isis area-tag interface network point-to-point

The **set protocols isis area-tag interface network point-to-point** command configures network type to ‘Point-to-Point’ (broadcast by default) .

The **delete protocols isis area-tag interface network point-to-point** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **network point-to-point**

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **network point-to-point**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.

Example

- Configure network type to ‘Point-to-Point’.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 network point-to-point
admin@PICOS# commit
```

set protocols isis area-tag interface passive

The **set protocols isis area-tag interface passive** command configures the specified layer 3 interface as passive IS-IS interface.

The **delete protocols isis area-tag interface passive** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **passive**

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **passive**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.

Example

- Configure the specified layer 3 interface as passive IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 passive
admin@PICOS# commit
```

set protocols isis area-tag interface password authentication-type

The **set protocols isis area-tag interface password authentication-type** command configures authentication type for the IS-IS interface.

The **delete protocols isis area-tag interface password** command deletes the configuration.

- Make sure that the authentication configuration per interface on both ends of IS-IS neighbor is consistent, otherwise neighbors cannot be established.
- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> **interface** <*interface-name*> **password**.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type for the IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag interface password authentication-key

The **set protocols isis area-tag interface password authentication-key** command configures authentication password for the IS-IS interface.

The **delete protocols isis area-tag interface password** command deletes the configuration.

- Make sure that the authentication configuration per interface on both ends of IS-IS neighbor is consistent, otherwise neighbors cannot be established.
- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> **interface** <*interface-name*> **password**.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **password authentication-key** <*password*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag interface priority

The **set protocols isis area-tag interface priority** command configures priority for Designated Router election.

The **delete protocols isis area-tag interface priority** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **priority** <*priority*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **priority**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
priority <*priority*>	Specifies the priority for Designated Router election. The value is an integer ranging from 0 to 127. The default value is 64. The higher the value, the higher the priority.

Example

- Configure the priority for Designated Router election.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 priority 85
admin@PICOS# commit
```

set protocols isis area-tag interface three-way-handshake

The **set protocols isis area-tag interface three-way-handshake** command is used to enable or disable the Three-Way Handshake for P2P adjacencies. Three-Way Handshake is enabled by default.
The **delete protocols isis area-tag interface three-way-handshake** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **three-way-handshake** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **three-way-handshake**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
three-way-handshake <**enable** | **disable**>	Enable or disable the Three-Way Handshake for P2P adjacencies. The value could be **enable** or **disable**. • **enable**: Enables the Three-Way Handshake for P2P adjacencies. • **disable**: Disables the Three-Way Handshake for P2P adjacencies. The default value is enable.

Example

- Disable the Three-Way Handshake for P2P adjacencies.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 three-way-handshake disable
admin@PICOS# commit
```

set protocols isis area-tag interface bfd

The **set protocols isis area-tag interface bfd** command configures parameters for Bidirectional Forwarding Detection (BFD) sessions on a specified IS-IS interface.

The **delete protocols isis area-tag interface bfd** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **bfd** [**profile** <text>]

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **bfd**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
profile <text>	Optional. Specifies the BFD profile name. The value is a string.

Example

- Configure parameters for Bidirectional Forwarding Detection (BFD) sessions on a specified IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 bfd profile profile1
admin@PICOS# commit
```

set protocols isis area-tag interface topology ipv6-unicast

The **set protocols isis area-tag interface topology ipv6-unicast** command enables an IPv6 unicast topology on a specified IS-IS interface.

The **delete protocols isis area-tag interface topology ipv6-unicast** command deletes the configuration.

To enable an IPv6 unicast topology on a specified IS-IS interface, users have to enable the global configuration (**set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast** [**overload**]) first.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **topology ipv6-unicast** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **topology ipv6-unicast**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
<**enable** | **disable**>	Enables or disables an IPv6 unicast topology on a specified IS-IS interface. The value could be **enable** or **disable**. • **enable**: Enables an IPv6 unicast topology on a specified IS-IS interface. • **disable**: Disables an IPv6 unicast topology on a specified IS-IS interface. The default value is enable.

Example

- Enable an IPv6 unicast topology on a specified IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 topology ipv6-unicast enable
admin@PICOS# commit
```

set protocols isis area-tag redistribute

The command **set protocols isis area-tag redistribute** redistributes routes of a specified type or protocol into IS-IS.

The command **delete protocols isis area-tag redistribute** removes this configuration.

Command Syntax

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute** <**ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2> metric**

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute** <**ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2> metric**

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing** | **ipv6-routing**>	Specifies the IP network type.
<**level-1** | **level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
bgp	Specifies the BGP routes for redistribution.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
ospf	Specifies the OSPF routes for redistribution.
ospf6	Specifies the OSPFv3 routes for redistribution.
rip	Specifies the RIP routes for redistribution.
ripng	Specifies the RIPng routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric <*metric*>	Optional. Specifies the route metric. The value is an integer that ranges from 0 to 16777215.
route-map <*route-map*>	Optional. Specifies the route map name for the route. The value is a string.

Example

- Configure IS-IS to redistribute BGP routes into IS-IS with metric 5.

```
admin@PICOS# set protocols isis area-tag instance1 redistribute ipv4-routing bgp level-1 metric 5
admin@PICOS# commit
```

set protocols isis traceoption events

The **set protocols isis traceoption events** command can be used to enable or disable IS-IS debugging for event tracing.

The **delete protocols isis traceoption events** command deletes the configuration.

Command Syntax

set protocols isis traceoption events

delete protocols isis traceoption events

Parameters

Null.

Example

- Enable IS-IS debugging for event tracing.

```
admin@PICOS# set protocols isis traceoption events
admin@PICOS# commit
```

set protocols isis traceoption adj-packets

The **set protocols isis traceoption adj-packets** command can be used to enable or disable IS-IS debugging for IS-IS Adjacency related packets.

The **delete protocols isis traceoption adj-packets** command deletes the configuration.

Command Syntax

set protocols isis traceoption adj-packets

delete protocols isis traceoption adj-packets

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS Adjacency related packets.

```
admin@PICOS# set protocols isis traceoption adj-packets
admin@PICOS# commit
```

set protocols isis traceoption route-events

The **set protocols isis traceoption route-events** command can be used to enable or disable IS-IS debugging for IS-IS Route related events.

The **delete protocols isis traceoption route-events** command deletes the configuration.

Command Syntax

set protocols isis traceoption route-events

delete protocols isis traceoption route-events

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS Route related events.

```
admin@PICOS# set protocols isis traceoption route-events
admin@PICOS# commit
```

set protocols isis traceoption snp-packets

The **set protocols isis traceoption snp-packets** command can be used to enable or disable IS-IS debugging for IS-IS CSNP/PSNP packets.
The **delete protocols isis traceoption snp-packets** command deletes the configuration.

Command Syntax

set protocols isis traceoption snp-packets
delete protocols isis traceoption snp-packets

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS CSNP/PSNP packets.

```
admin@PICOS# set protocols isis traceoption snp-packets
admin@PICOS# commit
```

run show isis summary

The **run show isis summary** command shows summary information about IS-IS.

Command Syntax

run show isis [**vrf** <*text*>**| vrf all**] **summary** [**json**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.

Example

- View the summary information of the IS-IS configuration.

```
admin@PICOS# run show isis summary
vrf             : default
Process Id      : 977
System Id       : 0000.0000.0004
Up time         : 00:31:32 ago
Number of areas : 2
Area instance1:
  Net: 34.0000.0000.0004.00
  TX counters per PDU type:
   LSP RXMT: 0
  RX counters per PDU type:
  Level-1:
    LSP0 regenerated: 7
         LSPs purged: 0
    SPF:
      minimum interval  : 44
    IPv4 route computation:
      last run elapsed  : 00:11:40 ago
      last run duration : 47 usec
      run count         : 6
  Level-2:
    LSP0 regenerated: 7
         LSPs purged: 0
    SPF:
      minimum interval  : 44
    IPv4 route computation:
      last run elapsed  : 00:11:40 ago
      last run duration : 21 usec
      run count         : 6
```

run show isis interface

The **run show isis interface** command displays information about layer 3 interfaces participating in IS-IS process.

Command Syntax

run show isis [vrf *<text>* **| vrf all] interface** *<text>* [**detail**] [**json**]

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name.
interface *<text>*	Specifies an interface name.

Example

- View information about layer 3 interfaces participating in IS-IS process.

```
admin@PICOS# run show isis interface vlan100
Area 1:
  Interface: vlan100, State: Up, Active, Circuit Id: 0x4c
    Type: lan, Level: L1L2, SNPA: 1c72.1dc9.1be1
    Level-1 Information:
      Metric: 10, Active neighbors: 1
      Hello interval: 3, Holddown count: 10 (pad)
      CNSP interval: 10, PSNP interval: 2
      LAN Priority: 64, is not DIS
    Level-2 Information:
      Metric: 10, Active neighbors: 1
      Hello interval: 3, Holddown count: 10 (pad)
      CNSP interval: 10, PSNP interval: 2
      LAN Priority: 64, is not DIS
    IP Prefix(es):
      1.1.1.1/24
    IPv6 Link-Locals:
      fe80::1e72:1d08:3c9:1be1/64
    IPv6 Prefixes:
      1000::1/64


admin@PICOS# run show isis interface
Area instance1:
  Interface   CircId   State    Type     Level
  vlan25      0x0      Config   p2p      L2
Area 1:
  Interface   CircId   State    Type     Level
  vlan10      0x4a     Up       lan      L1L2
  vlan100     0x4c     Up       lan      L1L2
  vlan200     0x4d     Up       lan      L1L2
```

run show isis database

The **run show isis database** command displays the Link State Database (LSDB) information of IS-IS.

Command Syntax

run show isis [vrf <*text*> **| vrf all**] **database** [**detail**] [**json**] [**lsp-id** <*lsp-id*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
lsp-id <*lsp-id*>	Optional. Specifies the LSP ID to be displayed. The value is in the format of xxxx.xxxx.xxxx.xx-xx. For example, 0460.0600.6004.00-00.

Example

- View the Link State Database (LSDB) information of IS-IS.

```
admin@PICOS# run show isis database
Area 1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xc721     542    1/0/0
PICOS.00-00               143   0x00000008  0x7627     699    1/0/0
PICOS.b1-00                51   0x00000003  0xe79f     728    1/0/0
PICOS.00-00               106   0x00000005  0xc718     394    1/0/0
PICOS.b3-00                51   0x00000004  0xba45     367    1/0/0
    5 LSPs

IS-IS Level-2 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xbf31     561    0/0/0
PICOS.00-00               143   0x00000008  0x6e37     719    0/0/0
PICOS.b1-00                51   0x00000003  0xdfaf     712    0/0/0
PICOS.00-00               106   0x00000005  0xbf28     450    0/0/0
PICOS.b3-00                51   0x00000004  0xb255     380    0/0/0
    5 LSPs



admin@PICOS# run show isis database detail
Area 1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xc721     508    1/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: localhost
  TE Router ID: 10.10.51.179
  Router Capability: 10.10.51.179 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  IPv4 Interface Address: 10.10.51.179
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 10.10.10.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/64 (Metric: 10)

PICOS.00-00               143   0x00000008  0x7627     665    1/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: PICOS
  TE Router ID: 10.10.51.53
```

```
  Router Capability: 10.10.51.53 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  Extended Reachability: 0000.0000.3333.b3 (Metric: 10)
  IPv4 Interface Address: 10.10.51.53
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 2.2.2.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/96 (Metric: 10)
  IPv6 Reachability: 2000::/96 (Metric: 10)

PICOS.b1-00                51   0x00000003  0xe79f     694    1/0/0
  Extended Reachability: 0000.0000.2222.00 (Metric: 0)
  Extended Reachability: 0000.0000.0004.00 (Metric: 0)

PICOS.00-00               106   0x00000005  0xc718     360    1/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: PICOS
  TE Router ID: 10.10.51.171
  Router Capability: 10.10.51.171 , D:0, S:0
  Extended Reachability: 0000.0000.3333.b3 (Metric: 10)
  IPv4 Interface Address: 10.10.51.171
  Extended IP Reachability: 2.2.2.0/24 (Metric: 10)
  IPv6 Reachability: 2000::/96 (Metric: 10)

PICOS.b3-00                51   0x00000004  0xba45     333    1/0/0
  Extended Reachability: 0000.0000.3333.00 (Metric: 0)
  Extended Reachability: 0000.0000.2222.00 (Metric: 0)

    5 LSPs

IS-IS Level-2 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xbf31     527    0/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: localhost
  TE Router ID: 10.10.51.179
  Router Capability: 10.10.51.179 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  IPv4 Interface Address: 10.10.51.179
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 10.10.10.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/64 (Metric: 10)
......
```

run show isis hostname

The **run show isis interface** command displays IS-IS hostname information.

Command Syntax

run show isis [vrf *<text>* **| vrf all] hostname**

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name.

Example

- View IS-IS hostname information.

```
admin@PICOS# run show isis hostname
vrf     : default
Level  System ID      Dynamic Hostname
2      0000.0000.2222 PICOS
2      0000.0000.3333 PICOS
     * 0000.0000.0004 localhost
```

run show isis neighbor

The **run show isis neighbor** command displays IS-IS neighbor information.

Command Syntax

run show isis [vrf <*text*> **| vrf all**] **neighbor** [**a-neighbor**<*text*>][**detail**] [**json**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
a-neighbor<*text*>	Specifies the system ID of an IS-IS neighbor.

Example

- View IS-IS neighbor information.

```
admin@PICOS# run show isis neighbor
Area 1:
  System Id           Interface   L  State        Holdtime SNPA
  PICOS               vlan100     1  Up            27       8cea.1b4b.7821
  PICOS               vlan100     2  Up            28       8cea.1b4b.7821



admin@PICOS# run show isis neighbor a-neighbor PICOS
Area 1:
 PICOS
    Interface: vlan100, Level: 1, State: Up, Expires in 28s
    Adjacency flaps: 1, Last: 3m34s ago
    Circuit type: L1L2, Speaks: IPv4, IPv6
    SNPA: 8cea.1b4b.7821, LAN id: PICOS.b1
    LAN Priority: 64, is DIS, DIS flaps: 1, Last: 3m34s ago
    Area Address(es):
      49.0001
    IPv4 Address(es):
      1.1.1.2
    IPv6 Address(es):
      fe80::8eea:1b10:14b:7821
    Global IPv6 Address(es):
      1000::2

 PICOS
    Interface: vlan100, Level: 2, State: Up, Expires in 29s
    Adjacency flaps: 1, Last: 3m35s ago
    Circuit type: L1L2, Speaks: IPv4, IPv6
    SNPA: 8cea.1b4b.7821, LAN id: PICOS.b1
    LAN Priority: 64, is DIS, DIS flaps: 1, Last: 3m35s ago
    Area Address(es):
      49.0001
    IPv4 Address(es):
      1.1.1.2
    IPv6 Address(es):
      fe80::8eea:1b10:14b:7821
    Global IPv6 Address(es):
      1000::2
```

run show isis route

The **run show isis route** command shows route information about IS-IS.

Command Syntax

run show isis [vrf *<text>***| vrf all]route** [**level-1**|**level-2**]

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name.
[**level-1**|**level-2**]	Optional. Specifies the routing information for the type of router to be displayed.

Example

- View the route information of IS-IS.

```
admin@PICOS# run show isis route level-1
Area 1:
IS-IS L1 IPv4 routing table:

 Prefix      Metric  Interface  Nexthop  Label(s)
 -------------------------------------------------
 1.1.1.0/24  20      vlan100    1.1.1.2  -
 2.2.2.0/24  20      vlan100    1.1.1.2  -

IS-IS L1 IPv6 routing table:

 Prefix     Metric  Interface  Nexthop                  Label(s)
 ------------------------------------------------------------------
 1000::/64  0       -          -                        -
 1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
 2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -


admin@PICOS# run show isis route
Area 1:
IS-IS L1 IPv4 routing table:

 Prefix         Metric  Interface  Nexthop  Label(s)
 ---------------------------------------------------
 1.1.1.0/24     20      vlan100    1.1.1.2  -
 2.2.2.0/24     20      vlan100    1.1.1.2  -
 10.10.10.0/24  0       -          -        -

IS-IS L1 IPv6 routing table:

 Prefix     Metric  Interface  Nexthop                  Label(s)
 ------------------------------------------------------------------
 1000::/64  0       -          -                        -
 1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
 2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -

IS-IS L2 IPv4 routing table:

 Prefix         Metric  Interface  Nexthop  Label(s)
 ---------------------------------------------------
 1.1.1.0/24     20      vlan100    1.1.1.2  -
 2.2.2.0/24     20      vlan100    1.1.1.2  -
 10.10.10.0/24  0       -          -        -

IS-IS L2 IPv6 routing table:
```

```
Prefix     Metric  Interface  Nexthop                   Label(s)
-----------------------------------------------------------------
1000::/64  0       -          -                         -
1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
```

run show isis topology

The **run show isis topology** command shows topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

Command Syntax

run show isis [vrf *<text>***| vrf all] topology [level-1|level-2]**

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies a VRF name.
[**level-1**|**level-2**]	Optional. Specifies the topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

Example

- View the topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

```
admin@PICOS# run show isis topology level-1
Area 1:
IS-IS paths to level-1 routers that speak IP
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1.1.1.0/24           IP internal  0                                     localhost(4)
10.10.10.0/24        IP internal  0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1.1.1.0/24           IP TE        20     PICOS                vlan100   PICOS(4)
2.2.2.0/24           IP TE        20     PICOS                vlan100   PICOS(4)

IS-IS paths to level-1 routers that speak IPv6
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1000::/64            IP6 internal 0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1000::/96            IP6 internal 20     PICOS                vlan100   PICOS(4)
2000::/96            IP6 internal 20     PICOS                vlan100   PICOS(4)


admin@PICOS# run show isis topology level-2
Area 1:
IS-IS paths to level-2 routers that speak IP
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1.1.1.0/24           IP internal  0                                     localhost(4)
10.10.10.0/24        IP internal  0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1.1.1.0/24           IP TE        20     PICOS                vlan100   PICOS(4)
2.2.2.0/24           IP TE        20     PICOS                vlan100   PICOS(4)

IS-IS paths to level-2 routers that speak IPv6
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1000::/64            IP6 internal 0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
```

```
PICOS               pseudo_TE-IS 20     PICOS               vlan100   PICOS(4)
PICOS               pseudo_TE-IS 20     PICOS               vlan100   PICOS(4)
PICOS               TE-IS        20     PICOS               vlan100   PICOS(2)
1000::/96           IP6 internal 20     PICOS               vlan100   PICOS(4)
2000::/96           IP6 internal 20     PICOS               vlan100   PICOS(4)
```

ACL Configuration Commands

This section contains descriptions of the ACL commands that this chapter references.

- set firewall filter description
- set firewall filter input interface
- set firewall time-range periodic start
- set firewall time-range periodic end
- run show timerange
- run show filter
- set firewall filter sequence then dscp
- set firewall filter sequence then action
- set firewall filter sequence from destination-port
- set firewall filter sequence from protocol ip
- set firewall filter sequence from protocol ospf
- set firewall filter sequence description
- set firewall filter output interface
- set firewall filter input vlan-interface
- set firewall filter sequence from protocol udp
- set firewall filter sequence from destination-address-ipv6
- set firewall filter sequence then forwarding-class
- set firewall filter sequence from protocol tcp flags
- set firewall filter sequence from protocol igmp
- set firewall filter output routed-interface
- set firewall filter sequence log interval
- set firewall filter sequence from source-port
- set firewall filter output vlan-interface
- set firewall filter sequence from destination-address-ipv4
- set firewall system-output disable
- set firewall filter sequence from ip trust-mode
- set firewall filter sequence from source-mac-address
- set firewall filter sequence from destination-mac-address
- set firewall filter sequence from protocol tcp
- set firewall filter sequence from ip value
- set firewall filter input routed-interface
- set firewall filter sequence from protocol icmp
- set firewall filter sequence from protocol others
- set firewall filter sequence from ether-type
- set firewall filter sequence from vlan
- set firewall filter sequence from source-address-ipv6
- set firewall filter sequence from source-address-ipv4

set firewall filter description

To configure the filter description, use the **set firewall filter description** command in L2/L3 configuration mode. To remove the filter desctiption, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **description** <*filter-description*>

delete firewall filter <*fileter-name*> **description**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
description <*filter-description*>	Filter description.

Example

- The following example configures the filter named *MyFilter* with the description *It's a test filter*.

```
admin@Switch# set firewall filter MyFilter description "It's a test filter"
admin@Switch# commit
```

- The folowing example removes the description of the filter *MyFilter*. Note that only the description is removed. The filter itself is not deleted by this command.

```
admin@Switch# delete firewall filter MyFilter description
Deleting:
   description: "\"It's a test filter\""
OK
admin@Switch# commit
```

set firewall filter input interface

The **set firewall filter input interface** command applies firewall filter to the incoming packets at an interface. To remove the input interface from the filter, use the **delete** format of the command.

Command Syntax

set firewall filter <*filer-name*> **input interface** <*interface-name*>
delete firewall filter <*filer-name*> **input interface** <*interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
interface <*interface-name*>	Specifies a switch interface. The value could be a physical interface, a logic interface or **inbound-control-plane**. For example, te-1/1/49, ae1. **Note:** When the interface name is configured to **inbound-control-plane**, it means applying firewall filter to the incoming packets directed to switch CPU. As this function is substituted by CoPP feature, the value **inbound-control-plane** will have no effect. For details of CoPP, please refer to CoPP Configuration Guide.

Example

- Set the firewall filter f1 at interface te-1/1/49.

```
admin@Switch# set firewall filter f1 input interface te-1/1/49
admin@Switch# commit
```

set firewall time-range periodic start

The **set firewall time-range periodic start** command configures the starting time of a time range.

The **delete firewall time-range periodic start** command deletes the configuration.

Command Syntax

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **start** <*starting-time*>

Parameters

Parameter	Description
time-range <*time-range-name***>**	Specifies the time range name. The value is a string in alpha-numeric format with no spaces.
periodic <*periodic*>	Specifies the periodic name. The value is an integer. Range: 0 to 9999.
<**daily**	**friday	monday	saturday	sunday	thursday	tuesday	wednesday	weekdays	weekend**>	Specifies the days of the week.
start <*starting-time*>	Specifies the starting time of a time range in 24-hour clock format. Format: HH:MM:SS.

Usage Guidelines

NOTEs:

- A pair of start time and end time forms a time range.
- Currently only one **periodic** can be configured under a **time range**. However, multiple time periods can be configured under one **periodic**. All the time periods under the same time range take effect.
- In the same **periodic**, you cannot configure **daily**, **weekdays**, **weekend** at the same time.

```
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays start 8:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays end 18:00:00
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily start 1:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily end 3:00:00
admin@Xorplus# commit
'daily', 'weekdays', 'weekend' should be configured separately in one periodic
Commit failed.
```

Example

- Configure a time range named timerange1234 of weekdays from 8:00:00 to18:00:00.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
admin@Xorplus# commit
```

set firewall time-range periodic end

The **set firewall time-range periodic end** command configures the ending time of a time range.

The **delete firewall time-range periodic end** command deletes the configuration.

Command Syntax

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **end** <*ending-time*>

Parameters

Parameter	Description
time-range <*time-range-name***>**	Specifies the time range name. The value is a string in alpha-numeric format with no spaces.
periodic <*periodic*>	Specifies the periodic name. The value is an integer. Range: 0 to 9999.
<**daily**	**friday	monday	saturday	sunday	thursday	tuesday	wednesday	weekdays	weekend**>	Specifies the days of the week.
end <*ending-time*>	Specifies the ending time of a time range in 24-hour clock format. Format: HH:MM:SS.

Usage Guidelines

NOTEs:

- A pair of start time and end time forms a time range.
- Currently only one **periodic** can be configured under a **time range**. However, multiple time periods can be configured under one **periodic**. All the time periods under the same time range take effect.
- In the same **periodic**, you cannot configure **daily**, **weekdays**, **weekend** at the same time.

```
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays start 8:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays end 18:00:00
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily start 1:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily end 3:00:00
admin@Xorplus# commit
'daily', 'weekdays', 'weekend' should be configured separately in one periodic
Commit failed.
```

Example

- Configure a time range named timerange1234 of weekday from 8:00:00 to18:00:00.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
admin@Xorplus# commit
```

run show timerange

The **run show timerange** command is used to view the time range configuration information.

Command Syntax

run show timerange [*<time-range-name>*]

Parameter

Parameter	Description
<time-range-name>	Optional. Specifies a time range name. The value is a string.

Example

- View the time range configuration information.

```
admin@Xorplus# run show timerange timerange4
TimeRange: timerange4
Periodic: 4
    Week: thursday, start:15:00:00, end:15:10:00

admin@Xorplus# run show timerange
TimeRange: time_range1
Periodic: 0
    Week: daily, start:16:10:00, end:16:15:00
TimeRange: time_range2
Periodic: 1
    Week: friday, start:05:00:00, end:05:10:00
    Week: monday, start:01:25:00, end:01:30:00
    Week: thursday, start:04:10:00, end:04:15:00
    Week: tuesday, start:15:53:00, end:15:54:00
    Week: wednesday, start:00:00:00, end:02:41:00
Periodic: 8881
    Week: friday, start:13:00:00, end:13:10:00
```

run show filter

The command displays information about all filters or a specified filter.

Command Syntax

run show filter [<*filter-name*>]

Parameters

Parameter	Description
<*filter-name*>	Optional. Specifies a filter name.

Example

• This example shows all filter information:

```
admin@XorPlus# run show filter
Filter: f1
Description: asa
Input interface: ge-1/1/1
run show
Filter: f2
Description:
Input interface: vlan2
Filter: f3
Description:
Output interface: ge-1/1/2
Filter: f4
Description:
Output interface: vlan2
• Show filter f1
XorPlus# run show filter f1
Filter: f1
Description: asa
Input interface: ge-1/1/1

```

- This example shows an ACL-based ERSPAN information:

```
admin@Xorplus# run show filter f1
Filter: f1
    Description:
    Sequence: 1
        Description:
        match counter:  751233 packets
        match-condition:
            protocol:                tcp
            source-address-ipv4:     1.1.1.100/32
        action: forward
```

```
        Erspan Output:
               state: UP
               source-ip: 172.1.1.100
               dest-ip: 192.1.1.100
               output-port: te-1/1/2
               tagged vlan:
               vrf:
               ttl: 255
        forwarding_class:
    Input interface: te-1/1/1
```

set firewall filter sequence then dscp

The **set firewall filter sequence then dscp** command remarks the DSCP priority in packets.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then dscp** <*dscp-value*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies a filter name. The value is a string. If the value is **copp**, it indicates a COPP configuration, please refer to set firewall filter copp sequence then dscp for details.
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
dscp <*dscp-value*>	Specifies a value to remark the DSCP priority in packets. The value is an integer in the range of 0 to 63.

Usage Guidelines

To provide differentiated services based on the DSCP priority, run this command to configure the device to remark the DSCP priority in IP packets in a traffic behavior. The DSCP remark function is enabled only when a remarked DSCP priority is set by the user.

Whether the DSCP remark is applied to the inbound or outbound direction on an interface, the device still processes outgoing packets based on the original priority value in the packets, but all the downstream Layer 3 devices processes the packets based on the remarked priority.

Example

- Remark the DSCP priority in packets to 20.

```
admin@Xorplus# set firewall filter f1 sequence 51 then dscp 20
```

set firewall filter sequence then action

To configure the next action for a filter sequence, use the **set firewall filter sequence then action** command in L2/L3 configuration mode.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then action** { **discard** | **forward** }

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
discard	Discard packets that meet all match conditions.
forward	Forward packets that meet all match conditions.

Examples

- The following example configures sequence 1 and 2 of the *MyFilter* filter to forward and discard matching packets, respectively.

```
admin@Switch# set firewall filter MyFilter sequence 1 then action forward
admin@Switch# set firewall filter MyFilter sequence 2 then action discard
admin@Switch# commit
```

set firewall filter sequence from destination-port

- To configure a filter sequence to match packets based on destination port, use the **set firewall filter sequence from destination-port** command in L2/L3 configuration mode. To remove the destination port, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from destination-port** <*port*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from destination-port**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
destination-port <*port*>	Destination port number or port number range, for example, 5000 or 7000..7050.

Example

- The following example configures sequence 2 of the *MyFilter* filter to match packets, which destination ports are in the 100-200 range:

```
admin@Switch# set firewall filter MyFilter sequence 2 from destination-port 100..200
admin@Switch# commit
```

- The following example removes the 100-200 port range from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from destination-port
Deleting:
   destination-port: 100..200
OK
admin@Switch# commit
```

set firewall filter sequence from protocol ip

To configure a filter sequence to match IP (Internet Porotocol) packets, use the **set firewall filter sequence from protocol ip** command in L2/L3 configuration mode. To remove IP packet matching from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol ip**
delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol ip**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match IP packets:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol ip
admin@Switch# commit
```

- The following example removes the condition that matches IP packets from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol ip
Deleting:
   protocol {
      ip {
      }
  }
OK
admin@Switch# commit
```

set firewall filter sequence from protocol ospf

To configure a filter sequence to match OSPF (Open Shortest Path First) protocol packets, use the **set firewall filter sequence from protocol ospf** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol ospf**
delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol ospf**

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match OSPF protocol packets:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol ospf
admin@Switch# commit
```

- The following example removes the condition from sequence 10 of the *MyFilter* fitler:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol ospf
Deleting:
  protocol {
     ospf {
     }
  }
OK
admin@Switch# commit
```

set firewall filter sequence description

To configure the filter sequence description, use the **set firewall filter sequence description** command in L2/L3 configuration mode. To remove the filter sequence description, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <sequence-*number*> **description** <*sequence-description*>
delete firewall filter <*filter-name*> **sequence** <*number*> **description**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*sequence-number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
description <*sequence-description*>	The sequence description.

Example

- The following example configures the description for sequence 10 of the *MyFilter* filter:

```
admin@Switch# set firewall filter MyFilter sequence 10 description "My filter sequence"
admin@Switch# commit
```

- The following example removes the description for sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 description
Deleting:
   description: "My filter sequence"
OK
admin@Switch# commit
```

set firewall filter output interface

To apply a filter to egress packets at an interface, use the **set firewall filter output interface** command in L2/L3 configuration mode. To remove the filter from an egress interface, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **output interface** <*interface-name*>
delete firewall filter <*filter-name*> **output interface** <*interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
output interface <*interface-name*>	Interface name.

Example

- The following example applies the *MyFilter* filter to egress packets on the *ge-1/1/2* interface:

```
admin@Switch# set firewall filter MyFiler output interface ge-1/1/2
admin@Switch# commit
```

- The following example removes the *MyFilter* filter from egress packets on the *ge-1/1/2* interface:

```
admin@Switch# delete firewall filter MyFiler output interface ge-1/1/2
Deleting:
   ge-1/1/2
OK
admin@Switch# commit
```

set firewall filter input vlan-interface

To apply the filter to ingress packets on a VLAN interface, use the **set firewall filter input vlan-interface** command in L2/L3 configuration mode. To remove the filter from ingress packets on a VLAN interface, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **input vlan-interface** <*vlan-interface-name*>
delete firewall filter <*filter-name*> **input vlan-interface** <*vlan-interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
vlan-interface <*vlan-interface-name*>	VLAN interface name.

Example

- The following example applies the *MyFilter* filter to ingress packets at the *vlan2* interface:

```
admin@Switch# set firewall filter MyFilter input vlan-interface vlan2
admin@Switch# commit
```

- The following example removes the *MyFilter* filter from ingress packets at the *vlan2* interface:

```
admin@Switch# delete firewall filter MyFilter input vlan-interface vlan2
Deleting:
   vlan2
OK
admin@Switch# commit
```

set firewall filter sequence from protocol udp

To configure a filter sequence to match packets with UDP (User Datagram Protocol) as Layer 4 protocol, use the **set firewall filter sequence from protocol udp** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** from of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol udp**

delete firewall filter *filter-name* **sequence** *number* **from protocol udp**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match packets carrying UDP as Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol udp
admin@Switch# commit
```

- The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol udp
Deleting:
   protocol {
      udp {
      }
  }
OK
admin@Switch# commit
```

set firewall filter sequence from destination-address-ipv6

To configure a filter sequence to match packets based on the destination IPv6 address, use the **set firewall filter sequence from destination-address-ipv6** command in L2/L3 configuration mode. To remove the destination IPv6 address, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from destination-address-ipv6** <*ipv6-address/mask*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from destination-address-ipv6**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
destination-address-ipv6 <*ipv6-address/mask*>	IPv6 address and prefix length.

Example

- The following example configures sequence 2 of the *MyFilter* filter to match packets with IPv6 destination address 2001::1/32:

```
admin@Switch# set firewall filter MyFilter sequence 2 from destination-address-ipv6 2001::1/128
admin@Switch# commit
```

- The following example removes IPv6 destination address 2001::1/32 from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from destination-address-ipv6
Deleting:
   destination-address-ipv6: 2001::1/128
OK
admin@Switch# commit
```

set firewall filter sequence then forwarding-class

The **set firewall filter sequence then forwarding-class** command sets forwarding class of ACL rule.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then forwarding-class** <*forwarding-class-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
forwarding-class <*forwarding-class-name* >	Specifies forwarding class name, the value is a string type, spaces are not allowed.

Usage Guidelines

After configuring a forwarding class, user could use the **set class-of-service forwarding-class local-priority** command to set mapping between forwarding class and local priority.

Example

- Set sequence number 51 to forwarding class class7.

```
admin@Xorplus# set firewall filter f1 sequence 51 then forwarding-class class7
admin@Xorplus# commit
```

set firewall filter sequence from protocol tcp flags

To configure a filter sequence to match packets with TCP as Layer 4 protocol and the specified TCP flag type, use the **set firewall filter sequence from protocol tcp flags** command in L2/L3 configuration mode.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol tcp flags** <*type*> { **true** | **false** }
delete firewall filter <*filter-name*> **sequence <***number*> **from protocol tcp flags** <*type*>

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
flags <*type*>	TCP flag type. Possible values are: **ack** **fin** **psh** **rst** **syn** **tcp-established** **tcp-initial urg**
true	The flag is set (1).
false	The flag is not set (0).

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match packets with TCP as the Layer 4 protocol and specified values for TCP flags:

```
admin@Switch# set firewall filter MyFilter sequence 1 from protocol tcp flags ack true
admin@Switch# set firewall filter MyFilter sequence 1 from protocol tcp flags psh false
admin@Switch# commit
```

- The following example removes both match conditions from sequence 1 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 1 from protocol tcp flags ack
Deleting:
   ack: true
OK
admin@Switch# delete firewall filter MyFilter sequence 1 from protocol tcp flags psh
```

```
Deleting:
   psh: false
OK
admin@Switch# commit
```

set firewall filter sequence from protocol igmp

To configure a filter sequence to match packets encapsulating IGMP as the Layer 4 protocol, use the **set firewall filter sequence from protocol igmp** command in L2/L3 configuration mode.

set firewall filter sequence from protocol icmp and **set firewall filter sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter sequence from protocol others** command with the protocol number.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol igmp**

delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol igmp**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.

Examples

- The following example configures sequence 10 of the filter named *MyFilter* to match packets with IGMP as the Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol igmp
admin@Switch# commit
```

set firewall filter output routed-interface

To apply a filter to egress packets at a routed interface, use the **set firewall filter output routed-interface** command in L2/L3 configuration mode. To remove the filter, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **output routed-interface** <*routed-interface-name*>
delete firewall filter <*filter-name*> **output routed-interface** <*routed-interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
routed-interface <*routed-interface-name*>	Routed interface name.

Example

- This example applies the *MyFilter* filter to egress packets at the routed interface *rif-ge3*:

```
admin@Switch# set firewall filter MyFilter output routed-interface rif-ge3
admin@Switch# commit
```

- This example removes the *MyFilter* filter from egress packets at the routed interface *rif-ge3*:

```
admin@Switch# delete firewall filter MyFilter output routed-interface rif-ge3
Deleting:
    ge3
OK
admin@Switch# commit
```

set firewall filter sequence log interval

To configure the log interval for a filter sequence, use the **set firewall filter sequence log interval** in L2/L3 configuration mode. To remove the log interval, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **log interval** <*time*>
delete firewall filter <*filter-name*> **sequence** <*number*> **log interval**

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
interval <*time*>	Log interval in seconds.

Example

- The following example configures sequence 10 of the *MyFilter* filter to record the log every 15 seconds:

```
admin@Switch# set firewall filter MyFilter sequence 10 log interval 15
admin@Switch# commit
```

- The following example removes the log interval from sequence 10 of *the MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 log interval
Deleting:
   interval: 15
OK
admin@Switch# commit
```

set firewall filter sequence from source-port

To configure a filter sequence to match packets with the specified source port, use the **set firewall filter sequence from source-port** command in L2/L3 configuration mode. To remove the match condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from source-port** <*port-number*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from source-port**

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
source-port <*port-number*>	Source port number.

Examples

- The following example configures sequence 2 of the *MyFilter* filter to match packets with source port in the 100-234 range:

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from source-port 100..234
admin@XorPlus# commit
```

- The following example removes the **souce-port** match condition from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from source-port
Deleting:
   source-port: 100..234
OK
admin@XorPlus# commit
```

set firewall filter output vlan-interface

To apply a filter to egress packets at a VLAN interface, use the **set firewall filter output vlan-interface** command in L2/L3 configuration mode. To remove the filter, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **output vlan-interface** <*vlan-interface-name*>
delete firewall filter <*filter-name*> **output vlan-interface** <*vlan-interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
output vlan-interface <*vlan-interface-name*>	VLAN interface name.

Example

- This example applies the *MyFilter* filter to egress packets at the VLAN interface *vlan2*:

```
admin@Switch# set firewall filter MyFilter output vlan-interface vlan2
admin@Switch# commit
```

- This example removes the *MyFilter* filter from egress packets at the VLAN interface *vlan2*:

```
admin@Switch# delete firewall filter MyFilter output vlan-interface vlan2
Deleting:
    vlan2
OK
admin@Switch# commit
```

set firewall filter sequence from destination-address-ipv4

To filter packets with a specific destination IP address, use the **set firewall filter sequence from destination-address-ipv4** command in L2/L3 configuration mode. To remove the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv4** <*address/mask*>
delete firewall filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv4**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*sequence-number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
destination-address-ipv4 <address/mask>	IPv4 subnet and subnet mask. For example, 10.1.1.0/24.

Example

- The following example configures sequence 1 of the *MyFilter* filter to drop packets to the destination IP address 192.168.1.1:

```
admin@Switch# set firewall filter MyFilter sequence 1 from destination-address-ipv4 192.168.1.1/32
admin@Switch# commit
```

- The following example prevents sequence 1 of the *MyFilter* filter from dropping packets based on destination IP packets:

```
admin@Switch# delete firewall filter MyFilter sequence 1 from destination-address-ipv4
Deleting:
   destination-address-ipv4: 192.168.1.1/32
OK
admin@Switch# commit
```

set firewall system-output disable

To prevent the switch from filtering packets originating from the switch itself, use the **set firewall system-output disable** command in L2/L3 configuration mode.

Command Syntax

set firewall system-out disable { **true** | **false** }

Parameters

Parameter	Description
true	Do not apply output filters to traffic from the system itself.
false	Apply output filters to traffic from the system itself.

Example

- This example configures the firewall to filter packets originating from the system:

```
admin@Switch# set firewall system-output disable true
admin@Switch# commit
```

set firewall filter sequence from ip trust-mode

To filter a packet with DSCP or IP Precendence in the packet header, use the **set firewall filter sequence from ip trust-mode** command in L2/L3 coniguration mode. To delete the configuration of firewall filter with DSCP or IP Precendence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from ip trust-mode** { **dscp** | **inet-precendence** }
delete firewall filter <*filter-name*> **sequence** <*number*> **from ip trust-mode**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
trust-mode { **dscp** | **inet-precendence** }	**dscp**: set the firewall filter condition to DSCP (Differentiated Services Code Point). **inet-precendence**: set the firewall filter condition to IP Precedence.

Usage Guidelines

When the firewall filter condition is configured to **dscp** or **inet-precendence**, you need to use the command set firewall filter sequence from ip value to configure the specific value of DSCP or IP Precedence.

These configurations are only used for filtering traffic based on DSCP or IP Precedence values in the packet header but have nothing to do with trust port.

Examples

- The following example configures sequence 2 of the *MyFilter* filter to trust DSCP value in the packet header:

```
admin@Switch# set firewall filter MyFilter sequence 2 from ip trust-mode dscp
admin@Switch# commit
```

- The following example removes the DSCP value from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from ip trust-mode
Deleting:
   trust-mode: "dscp"
OK
admin@XorPlus# commit
```

set firewall filter sequence from source-mac-address

To configure a filter sequence to match packets with the specified source MAC address, use the **set firewall filter sequence from source-mac-address** command in L2/L3 configuration mode.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from source-mac-address** <*mac-address*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from source-mac-address**

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
source-mac-address <*mac-address*>	Source MAC address.

Examples

- The following example configures seqence 2 of the *MyFilter* filter to match packets with the source MAC address 11:22:33:44:55:66:

```
admin@Switch# set firewall filter MyFilter sequence 2 from source-mac-address 11:22:33:44:55:66
admin@Switch# commit
```

- The following example removes the match condition from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from source-mac-address
Deleting:
   source-mac-address: 11:22:33:44:55:66
OK
admin@Switch# commit
```

set firewall filter sequence from destination-mac-address

To configure a filter sequence to match packets based on destination MAC address, use the **set firewall filter sequence from destination-mac-address** command in L2/L3 configuration mode. To remove the destination MAC address, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from destination-mac-address** <*mac-address*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from destination-mac-address**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
destination-mac-address <*mac-address*>	Destination MAC address.

Example

- The following example configures sequence 2 of the *MyFilter* filter to match packets with destination MAC address 44:44:44:44:44:44.

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from destination-mac-address 44:44:44:44:44:44
admin@Switch# commit
```

- The following example removes the destination MAC address 44:44:44:44:44:44 from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from destination-mac-address
Deleting:
   destination-mac-address: 44:44:44:44:44:44
OK
admin@Switch# commit
```

set firewall filter sequence from protocol tcp

To configure a filter sequence to match packets with TCP (Transmission Control Protocol) as the Layer 4 protocol, use the **set firewall filter sequence from protocol tcp** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol tcp**
delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol tcp**

Parameters

Parameter	Description
filter <*filter-name*>**>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match packets carrying TCP as the Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol tcp
```

- The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
Deleting:
   protocol {
       tcp {
      }
  }
OK
```

set firewall filter sequence from ip value

To configure a filter sequence to match packets based on DSCP or IP Precendence values, use the **set firewall filter sequence from ip value** command in L2/L3 configuration mode.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from ip value** <*value*>

delete firewall filter <*filter-name*> **sequence** <*number*> **from ip value**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
value <*value*>	DSCP or IP Precendence value, according to the trust mode configured with the set firewall filter sequence from ip trust-mode command. The range is 0-7 for IP Precedence, and 0-63 for DSCP.

Examples

- The following example configures the trust mode for sequence 2 of *MyFilter* filter to DSCP. The DSCP value used to match packets is then set to 2.

```
admin@Switch# set firewall filter MyFilter sequence 2 from ip trust-mode dscp
admin@Switch# set firewall filter MyFilter sequence 2 from ip value 2
admin@Switch# commit
```

- The following example removes the trust mode and DSCP value from sequence 2 of *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from ip
Deleting:
   ip {
       trust-mode: "dscp"
       value: 2
   }
OK
admin@Switch# commit
```

set firewall filter input routed-interface

To apply the filter to ingress packets on a routed interface, use the **set firewall filter input routed-interface** command in L2/L3 configuration mode. To remove the filter from ingress packets on a routed interface, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **input routed-interface** <*routed-interface-name*>
delete firewall filter <*filter-name*> **input routed-interface** <*routed-interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
routed-interface <*routed-interface-name*>	Routed interface name.

Example

- The following example applies the *MyFilter* filter to ingress packets at the *rif-ge3* interface:

```
admin@Switch# set firewall filter MyFilter input routed-interface rif-ge3
admin@Switch# commit
```

- The following example removes the *MyFilter* filter from ingress packets at the rif-ge3 interface:

```
admin@Switch# delete firewall filter MyFilter input routed-interface rif-ge3
Deleting:
   ge3
OK
admin@Switch# commit
```

set firewall filter sequence from protocol icmp

To configure a filter sequence to match ICMP (Internet Control Message Protocol) packets, use the **set firewall filter sequence from protocol icmp** command in L2/L3 configuration mode.

set firewall filter sequence from protocol icmp and **set firewall filter sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter sequence from protocol others** command with the protocol number.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol icmp** [**type** <*type*> | **code** <*code*>]
delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol icmp** [**type** | **code**]

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
type <*type*>	ICMP type. The range is 0-254.
code <*code*>	ICMP code. The range is 0-254.

Examples

- The following example configures sequence 10 of the *MyFilter* filter to match packets with 0 as the ICMP code and 24 as the ICMP type:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol icmp code 0
admin@Switch# set firewall filter MyFilter sequence 10 from protocol icmp type 24
admin@Switch# commit
```

- The following example removes the match conditions from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol icmp code
Deleting:
   code: 0
OK
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol icmp type
Deleting:
   type: 24
OK
admin@Switch# commit
```

set firewall filter sequence from protocol others

To configure a filter sequence to match packets with the specified Layer 4 protocol number, use the **set firewall filter sequence from protocol others** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from protocol others** <*protocol-number*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from protocol others**

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
others <*protocol-number*>	Layer 4 protocol number. The range is 0-255.

Examples

- This example configures sequence 10 of the *MyFilter* filter to match packets carrying Layer 4 protocol number 21:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol others 21
admin@Switch# commit
```

- The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol others
admin@Switch# commit
```

set firewall filter sequence from ether-type

To configure a filter sequence to match packets based on the EtherType field in the Ethernet frame, use the **set firewall filter sequence from ether-type** command in L2/L3 configuration mode. To remove the EtherType field from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from ether-type** <*ether-type*>
delete firewall filter *filter-name* **sequence** *number* **from ether-type**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
ether-type <*ether-type*>	Ether-type value in decimal form. The range is 0-65535.

Example

- The following example configures sequence 2 of the *MyFilter* filter to match frames with EtherType value 0x0800 (2048 decimal):

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from ether-type 2048
admin@XorPlus# commit
```

- The following example removes the EtherType value from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from ether-type
Deleting:
   ether-type: 2048
OK
admin@XorPlus# commit
```

set firewall filter sequence from vlan

To configure a filer sequence to filter packets in a specific VLAN, use the **set firewall filter sequence from vlan** command in L2/L3 configuration mode.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **from vlan** <*vlan-id*>
delete firewall filter <*filter-name*> **sequence** <*number*> **from vlan**

Parameters

Parameter	Description
filter <*filter-name***>**	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
vlan <*vlan-id*>	VLAN identifier. The range is 1-4094.

Examples

- The following example applies sequence 2 of *MyFilter* filter to VLAN 3:

```
admin@Switch# set firewall filter MyFilter sequence 2 from vlan 3
admin@Switch# commit
admin@Switch# delete firewall filter MyFilter sequence 2 from vlan
Deleting:
 vlan: 2

OK
admin@Switch# commit
```

set firewall filter sequence from source-address-ipv6

To configure a filter sequence to match packets with specified destination IPv6 address, use the **set firewall filter sequence from source-address-ipv6** command in L2/L3 configuration mode. To remove the condition, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-address-ipv6** *address/prefix-length*
delete firewall filter *filter-name* **sequence** *number* **from source-address-ipv6**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
source-address-ipv6 <*address/prefix-length*>	IPv6 address / prefix length

Examples

- The following example configures sequence 2 of the *MyFilter* filter to match packets with source IPv6 address is 2001::1:

```
admin@Switch# set firewall filter MyFilter sequence 2 from source-address-ipv6 2001::1/128
admin@Switch# commit
```

- The following example removes the match condition from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from source-address-ipv6
Deleting:
   source-address-ipv6: 2001::1/128
OK
admin@Switch# commit
```

set firewall filter sequence from source-address-ipv4

To configure a filter sequence to match packets with specified source IP address, use the **set firewall filter sequence from source-address-ipv4** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-address-ipv4** <*address/prefix-length*>
delete firewall filter *filter-name* **sequence** *number* **from source-address-ipv4**

Parameters

Parameter	Description
filter <*filter-name*>	Filter name.
sequence <*number*>	The sequence number, smaller values representing higher priorities. The range is 0-9999.
source-address-ipv4 <*address/prefix-length*>	IPv4 address / prefix length

Examples

- The following example configures sequence 1 of the *MyFilter* filter to match packets with source address 192.168.1.1:

```
admin@Switch# set firewall filter MyFilter sequence 1 from source-address-ipv4 192.168.1.1/32
admin@Switch# commit
```

- The following example removes the condition from sequence 1 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 1 from source-address-ipv4
Deleting:
   source-address-ipv4: 192.168.1.1/32
OK
admin@Switch# commit
```

QoS Configuration Commands

This section contains descriptions of the Layer2 and Layer3 QoS configuration commands that this chapter references.

- set class-of-service forwarding-class local-priority
- set class-of-service scheduler mode
- set class-of-service interface default-priority
- set class-of-service classifier forwarding-class code-point
- set class-of-service interface classifier
- set class-of-service classifier
- set class-of–service classifier forwarding-class
- set class-of-service classifier trust-mode
- set class-of-service scheduler guaranteed-rate
- set class-of-service scheduler-profile forwarding-class scheduler
- set class-of-service scheduler weight
- set class-of-service easy-ecn mode
- set class-of-service interface scheduler-profile
- set class-of-service scheduler max-rate
- run show class-of-service interface
- CoPP Commands
  - set class-of-service scheduler max-bandwidth-pps
  - set class-of-service scheduler min-bandwidth-pps
  - set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
  - set class-of-service scheduler weight (CoPP)
  - set firewall filter copp sequence from destination-address-ipv4
  - set firewall filter copp sequence from destination-address-ipv6
  - set firewall filter copp sequence from destination-mac-address
  - set firewall filter copp sequence from destination-port
  - set firewall filter copp sequence from ether-type
  - set firewall filter copp sequence from protocol
  - set firewall filter copp sequence from source-address-ipv4
  - set firewall filter copp sequence from source-address-ipv6
  - set firewall filter copp sequence from source-mac-address
  - set firewall filter copp sequence from source-port
  - set firewall filter copp sequence from vlan
  - set firewall filter copp sequence then forwarding-class
  - set firewall filter copp sequence then dscp
  - run show copp bandwidth
  - run show copp statistics
  - run show interface stm
  - run clear copp statistics
  - set class-of-service forwarding-class local-priority (CoPP)
  - run show filter copp
- Buffer Management Commands
  - set interface ethernet-switching-options buffer egress-queue shared-ratio
  - set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
  - run show interface egress-buffer
  - run show interface gigabit-ethernet egress-queues
- Interface-based Rate Limiting Commands
  - set interface gigabit-ethernet rate-limiting ingress kilobits
  - set interface gigabit-ethernet rate-limiting ingress ratio
  - set interface gigabit-ethernet rate-limiting ingress burst
  - set interface gigabit-ethernet rate-limiting egress kilobits
  - set interface gigabit-ethernet rate-limiting egress ratio
  - set interface gigabit-ethernet rate-limiting egress burst
- ACL-based Traffic Policer Commands
  - set firewall policer if-exceeding count-mode
  - set firewall policer if-exceeding rate-limit
  - set firewall policer if-exceeding burst-limit
  - set firewall filter sequence then policer
  - set firewall policer if-exceeding action discard
  - run show policer
- PFC Commands
  - set class-of-service pfc-profile code-point drop
  - set class-of-service interface pfc-profile
  - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed
  - set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio

- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset
- set interface ethernet-switching-options buffer service-pool threshold
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom
- set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio
- set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold
- set class-of-service pfc-watchdog granularity
- set class-of-service pfc-watchdog restore-action
- set class-of-service pfc-watchdog code-point detect-interval
- set class-of-service pfc-watchdog code-point restore-interval
- set class-of-service interface pfc-watchdog code-point enable
- set class-of-service pfc-watchdog threshold period
- set class-of-service pfc-watchdog threshold count
- set class-of-service interface pfc-watchdog restore-mode
- run clear class-of-service interface pfc-watchdog auto
- run clear class-of-service interface pfc-watchdog manual
- run show pfc-watchdog stats
- run show pfc-watchdog config
- run show interface gigabit-ethernet ingress-buffer
- run show interface gigabit-ethernet egress-buffer
- set class-of-service interface pfc-uplink-group
- set class-of-service pfc-uplink-group original-dscp to-code-point
- set class-of-service pfc-uplink-group original-dscp dscp

set class-of-service forwarding-class local-priority

User can configure the local-priority for a special forwarding-class. The name of a forwarding-class is optionally implemented.

Command Syntax
set class-of–service forwarding-class <*forwarding-class-name*> **local-priority** <*int*>
delete class-of–service forwarding-class <*forwarding-class-name*> **local-priority**

Parameters

Parameter	Description
forwarding-class <*forwarding-class-name*>	Name of forwarding class.
local-priority <*int*>	Local priority,the valid local priority numbers range 0-7. Default value: 0

NOTE:
On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.

Example
• This example creates a forwarding-class f1and the local priority is 1.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 1
admin@XorPlus# commit
```

set class-of-service scheduler mode

User can configure a scheduler with SP, WEQ or WRR mode.

Command Syntax

set class-of–service scheduler <*scheduler-name*> **mode** {**SP | WEQ | WRR**}

delete class-of–service scheduler <*scheduler-name*> **mode**

Parameters

Parameter	Description
scheduler <*schedule-name*>	Queue scheduler configuration, it is optionally implemented.
mode {**SP	WEQ	WRR**}	Specifies the queque scheduler with mode SP, WEQ or WRR.

Example

- This example creates queue scheduler s1 with SP mode.

```
admin@XorPlus# set class-of-service scheduler s1 mode SP
admin@XorPlus# commit
```

set class-of-service interface default-priority

User can configure a default priority for incoming packets on a port. The default-priority acts on incoming packets without a special field which is dscp, ieee-802.1 or inet-precedence.

For example, when trust mode is dscp on an interface, if the incoming packets can‘t match dscp field, these packets will be transmitted by default-priority configured in the interface. Otherwise, these packets will be transmitted by dscp value.

Traffic class for default priority:

	Untrusted	CoS Trusted	ToS Trusted	DSCP Trusted
Untagged Non-IP	Default CoS (port)	Default CoS (port)	Default ToS (port)	Default DSCP (port)
Untagged IP	Default CoS (port)	Default CoS (port)	ToS (packet)	DSCP (packet)
Tagged Non-IP	Default CoS (port)	CoS (packet)	Default ToS (port)	Default DSCP (port)
Tagged IP	Default CoS (port)	CoS (packet)	ToS (packet)	DSCP (packet)

Command Syntax

set class-of–service interface <*port*> **default-priority** <*default-priority-type*> <*default-priority-int*>

delete class-of–service interface <*port*> **default-priority** <*default-priority-type*>

Parameters

Parameter	Description
interface <*port*>	Gigabit Ethernet Interface. e.g. ge-1/1/1.
default-priority <default-priority-type> <*default-priority-int*>	<*default-priority-type*>: the type of default priority, which can be dscp, ieee 802.1p or inet-precedence. The default value is ieee 802.1p. <*default-priority-int*>: the value of default priority, the valid range is 0~7 for ieee-802.1 and inet-precedence, 0~63 for dscp. The default value is 0 for dscp, ieee 802.1p or inet-precedence.

Example

- When not configuring any trust mode, configure default priority dscp 16 on ge-1/1/1.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 default-priority dscp 16
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
```

```
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 16
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

- When trust mode is dscp, configure default priority dscp 16 on ge-1/1/2.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode dscp
admin@XorPlus# set class-of-service interface te-1/1/2 classifier c1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface te-1/1/2
Interface : te-1/1/2
trust mode : dscp
Default ieee-802.1 : 0
Default dscp : 16
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                     0,1,2,3,4,5,6,7
1                SP,0kbps                     8,9,10,11,12,13,14,15
2                SP,0kbps                     16,17,18,19,20,21,22,23
3                SP,0kbps                     24,25,26,27,28,29,30,31
4                SP,0kbps                     32,33,34,35,36,37,38,39
5                SP,0kbps                     40,41,42,43,44,45,46,47
6                SP,0kbps                     48,49,50,51,52,53,54,55
7                SP,0kbps                     56,57,58,59,60,61,62,63
```

set class-of-service classifier forwarding-class code-point

User can configure a name for a classifier. This name can be applied in an input interface.

Command Syntax

set class-of–service classifier <*classifier-name*> **forwarding-class** <*forwarding-class-name*> **code-point** <*int*>

delete class-of–service classifier <*classifier-name*> **forwarding-class** <*forwarding-class-name*> **code-point** <*int*>

Parameters

Parameter	Description
classifier <*classifier-name*>	Classifier configuration. It is optionally implemented.
forwarding-class <*forwarding-class-name*>	Name of forwarding class
code-point <*int*>	Code-point , the valid range is 0~7 for ieee-802.1 and inet-precedence, 0~63 for dscp.

Example

- This example creates a classifier c1 with forwarding-class f1 and code-point 3

```
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 3
admin@XorPlus# commit
```

set class-of-service interface classifier

User can configure a classifier for port.

Command Syntax

set class-of–service interface <*port*> **classifier** <*classifier-name*>

delete class-of–service interface <*port*>

Parameters

Parameter	Description
interface <*port*>	GigabitEthernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1.
classifier <*classifier-name*>	Classifier configuration. It is optionally implemented.

Example

• This example creates classifier for port ge-1/1/1.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# commit
```

set class-of-service classifier

User can configure classifier-name for a classifier, and the name is optionally implemented.

Command Syntax
set class-of–service classifier <*classifier-name*>
delete class-of–service classifier

Parameters

Parameter	Description
classifier <*classifier-name*>	Classifier configuration. It is optionally implemented.

Example
• This example creates classifier c1:

```
admin@XorPlus# set class-of-service classifier c1
admin@XorPlus# commit
```

set class-of–service classifier forwarding-class

The **set class-of–service classifier forwarding-class** command configures a name for a forwarding class. This name can be applied in an input interface.

The **delete class-of–service classifier forwarding-class** command deletes the configuration.

Command Syntax

set class-of–service classifier <*classifier-name*> **forwarding-class** <*forwarding-class-name*>

delete class-of–service classifier <*classifier-name*> **forwarding-class** <*forwarding-class-name*>

Parameters

Parameter	Description
classifier <*classifier-name*>	Classifier configuration. It is optionally implemented.
forwarding-class <*forwarding-class-name*>	Name of forwarding class

Example

- This example creates a classifier c1 with forwarding-class f1.

```
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1
admin@XorPlus# commit
```

set class-of-service classifier trust-mode

User can configure classifier-name for a classifier, and the name is optionally implemented.
The value of trust-mode can be DSCP, IEEE 802.1p, or inet-precedence.

Command Syntax
set class-of–service classifier <*classifier-name*> **trust-mode** <*trust-mode*>
delete class-of–service classifier <*classifier-name***> trust-mode**

Parameters

Parameter	Description
classifier <*classifier-name* >	Classifier configuration. It is optionally implemented.
trust-mode <*trust-mode* >	Priority based. The value of trust-mode can be DSCP, IEEE 802.1p, or inet-precedence.

Example
• This example creates classifier c1 based on the trust-mode of DSCP:

```
admin@XorPlus# set class-of-service classifier c1 trust-mode dscp
admin@XorPlus# commit
```

• This example creates classifier c2 based on the trust-mode of IEEE 802.1p:

```
admin@XorPlus# set class-of-service classifier c2 trust-mode ieee 802.1p
admin@XorPlus# commit
```

• This example creates classifier c3 based on the trust-mode of inet-precedence:

```
admin@XorPlus# set class-of-service classifier c3 trust-mode inet-precedence
admin@XorPlus# commit
```

set class-of-service scheduler guaranteed-rate

User can configure the minimum guaranteed bandwith for WFQ queue.

Command Syntax

set class-of–service scheduler <*scheduler-name*> **guaranteed-rate** <*guaranteed-rate*>

delete class-of–service scheduler <*scheduler-name*> **guaranteed-rate**

Parameters

Parameter	Description
scheduler <*schedule-name*>	Queue scheduler configuration, it is optionally implemented.
guaranteed-rate <*guaranteed-rate*>	The minimum guaranteed bandwidth, only for WFQ. The valid guaranteed-rate range 8-40000000.

Example

- This example creates scheduler s1 with the minimum guaranteed bandwitdth 100.

```
admin@XorPlus# set class-of-service scheduler s1 guaranteed-rate 100
admin@XorPlus# commit
```

set class-of-service scheduler-profile forwarding-class scheduler

User can configure a schedule of queue and a forwarding class for a special scheduler-profile. This scheduler-profile can be applied on an interface.

Command Syntax

set class-of–service scheduler-profile <*scheduler-profile-name*> **forwarding-class** <*forwarding-class-name*> **scheduler** <*scheduler-name*>

delete class-of–service scheduler-profile <*scheduler-profile-name*> **forwarding-class** <*forwarding-class-name*> **scheduler**

Parameter

Parameter	Description
scheduler-profile <*scheduler-profile-name*>	Name of scheduler profile.
forwarding-class <*forwarding-class-name*>	Name of forwarding class.
scheduler <*scheduler-name*>	Queue scheduler configuration.

Example

- This example creates a scheduler-profile p1 with the forwarding-class f1 and the scheduler s1.

```
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f1 scheduler s1
admin@XorPlus# commit
```

set class-of-service scheduler weight

User can configure a scheduling weight of associated queues.

Command Syntax

set class-of–service scheduler <*scheduler-name*> **weight** <*weight-id*>

delete class-of–service scheduler <*scheduler-name*> **weight**

Parameters

Parameter	Description
scheduler <*schedule-name*>	Queue scheduler configuration. It is optionally implemented.
weight <*weight-id*>	The scheduling weight of associated queues. The valid weight numbers range 0-15.

Example

This example creates a scheduling weight of associated queues.

```
admin@XorPlus# set class-of-service scheduler s1 weight 3
admin@XorPlus# commit
```

set class-of-service easy-ecn mode

The **set class-of-service easy-ecn mode** command enables Easy ECN globally and choose the appropriate mode based on your needs. The mode **throughput-first** prioritizes maximizing the amount of data transferred across the network. The mode **latency-first** prioritizes minimizing latency, ensuring that packets experience the least possible delay. By default, Easy ECN function is disabled.

The **delete class-of-service easy-ecn mode** command deletes the configuration.

Command Syntax

set class-of-service easy-ecn mode <throughput-first | latency-first>

delete class-of-service easy-ecn mode

Parameter

Parameter	Description
mode <throughput-first | latency-first>	Specifies Easy ECN mode. The value could be **throughput-first** or **latency-first**. • **throughput-first**: prioritizes maximizing the amount of data transferred across the network. • **latency-first**: prioritizes minimizing latency, ensuring that packets experience the least possible delay.

Usage Guidelines

Class of Service (CoS) allows network administrators to manage and prioritize different types of traffic. ECN is a mechanism that helps manage network congestion by marking packets rather than dropping them when congestion occurs. This allows the sender to reduce its transmission rate before packets are dropped. Easy ECN simplifies the configuration and implementation of ECN, making it easier to deploy congestion control.

In this configuration, the mode "**throughput-first**" means that the primary goal of the CoS is to maximize data throughput (the total amount of data transferred across the network in a given period of time). This prioritization is beneficial in scenarios where achieving the highest possible data transfer rate is the main objective, such as in file transfers, content delivery, or data backup operations. The system will aim to maximize the volume of data transmitted, even if that means slightly higher latency or delay.

The mode "**latency-first**" means that the system will prioritize minimizing latency (the time it takes for a data packet to travel from source to destination) over other factors like throughput. This mode is suitable for latency-sensitive applications, such as VoIP (Voice over IP), video conferencing, or online gaming, where minimizing delay is crucial to maintaining performance quality.

Table 1 below shows ECN threshold and marking probability values for throughput-first and latency-first modes.

Table 1. ECN Threshold and Marking Probability: Throughput-First vs. Latency-First

Easy ECN Mode	ECN Threshold and Marking Probability	Tomahawk3	Trident3-X5 Trident3-X7	Tomahawk5
throughput-first	min_thresh (Bytes)	5,080,000	2,560,000	2,540,000

	max_thresh (Bytes)	25,400,000	12,800,000	12,700,000
	drop_probability	20%	20%	20%
latency-first	min_thresh (Bytes)	508,000	256,000	254,000
	max_thresh (Bytes)	2,540,000	1,280,000	1,270,000
	drop_probability	20%	20%	20%

Example

- Configure easy ECN mode to **throughput-first**.

```
admin@PICOS# set class-of-service easy-ecn mode throughput-first
admin@PICOS# commit
```

set class-of-service interface scheduler-profile

The **set class-of–service interface scheduler-profile** command applies scheduler profile at a switch physical interface.

Command Syntax

set class-of–service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>
delete class-of–service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies a switch physical interface. For example, te-1/1/49. **Note:** When the interface name is configured to **inbound-control-plane**, it means applying firewall filter to the incoming packets directed to switch CPU. As this function is substituted by CoPP feature, the value **inbound-control-plane** will have no effect. For details of CoPP, please refer to CoPP Configuration Guide.
scheduler-profile <*scheduler-profile-name*>	Specifies scheduler profile name, the value is a string type, spaces are not allowed.

Example

- Configure scheduler-profile p1 for port ge-1/1/1.

```
admin@Switch# set class-of-service interface ge-1/1/1 scheduler-profile p1
```

set class-of-service scheduler max-rate

The **set class-of-service scheduler max-rate** command sets the maximum rate for an interface queue.

The **delete class-of-service scheduler max-rate** command deletes the configuration.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **max-rate** <*value*>

set class-of-service scheduler <*scheduler-name*> **max-rate**

Parameters

Parameter	Description
scheduler <*scheduler-name*>	Specifies a scheduler name, the value is a string, spaces are not allowed.
max-rate <*value*>	Specifies the maximum rate of an interface queue. The value is an integer, in kbit/s.

Usage Guidelines

Configure the maximum rate on the physical interface egress queue of the packet to adjust the sending rate of the interface, thus preventing congestion on the downstream device. When the transmit rate of packets exceeds the queue-based rate limit, the packets will be discarded.

NOTE:

If both queue-based rate limiting and interface-based rate limiting (configured by the command **set interface gigabit-ethernet** <*port*> **rate-limiting** <**ingress** | **egress**> **kilobits** <*kilobits-ps*>) are configured on an interface, the smaller value of the two will be used for rate limiting.

Example

- Set the maximum rate of 30000 kbit/s for scheduler s3.

```
admin@Xorplus# set class-of-service scheduler s3 max-limit 30000
```

run show class-of-service interface

The **run show class-of-service** command displays information about QoS configured on switch. User can display the interface, trust-mode, local-priority, queue-schedule, and the code-point information. The default queue-schedule is SP.

Command Syntax

run show class-of-service interface <*interface-name***>**

Parameters

Parameter	Description
Interface <*interface-name***>**	Specifies the interface name.

Example

• Show the information of class-of-service on interface te-1/1/4.

```
admin@PICOS# run show class-of-service interface te-1/1/4
Interface : te-1/1/4

802.1P         Priority Flow Control    RxPFC              TxPFC
-----------    ---------------------    ---------------    ---------------
0              false                    0                  0
1              false                    0                  0
2              false                    0                  0
3              false                    0                  0
4              false                    0                  0
5              false                    0                  0
6              false                    0                  0
7              false                    0                  0
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   --------------------------   ------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

CoPP Commands

This section contains descriptions of the CoPP CLI commands.

Although the realization and commands of CoPP use the QoS module of CoS (Class of Service) and Firewall Filter Rule, but CoPP has its own command line with a fixed keyword **copp**, distinguishing it from the ACL feature.

- run clear copp statistics
- run show copp bandwidth
- run show copp statistics
- run show filter copp
- run show interface stm
- set class-of-service forwarding-class local-priority (CoPP)
- set class-of-service scheduler max-bandwidth-pps
- set class-of-service scheduler min-bandwidth-pps
- set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
- set class-of-service scheduler weight (CoPP)
- set firewall filter copp sequence from destination-address-ipv4
- set firewall filter copp sequence from destination-address-ipv6
- set firewall filter copp sequence from destination-mac-address
- set firewall filter copp sequence from destination-port
- set firewall filter copp sequence from ether-type
- set firewall filter copp sequence from protocol
- set firewall filter copp sequence from source-address-ipv4
- set firewall filter copp sequence from source-address-ipv6
- set firewall filter copp sequence from source-mac-address
- set firewall filter copp sequence from source-port
- set firewall filter copp sequence from vlan
- set firewall filter copp sequence then dscp
- set firewall filter copp sequence then forwarding-class

set class-of-service scheduler max-bandwidth-pps

The **set class-of-service scheduler max-bandwidth-pps** command sets the maximum bandwidth for a CPU queue.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **max-bandwidth-pps** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
max-bandwidth-pps <*value*>	Specifies the maximum bandwidth for a CPU queue. The value is an integer. The lower limit of max-bandwidth-pps is 0 and the upper limit of max-bandwidth-pps is the maximum bandwidth that the CPU can receive.

Usage Guidelines

If there is heavy traffic load on the interface caused by malicious attacks or network exceptions, the CPU is overloaded and services are interrupted. User can set a maximum bandwidth value for a CPU queue on the interface to control this problem.

The upper limit of max-bandwidth-pps is different on different platforms. If the configured max-bandwidth-pps value exceeds the maximum bandwidth that the CPU can receive, an error message is displayed with the range of the device supported max-bandwidth-pps. The following shows an example.

```
admin@Xorplus# set class-of-service scheduler s1 max-bandwidth-pps 40000
admin@Xorplus# commit
The maximum bandwidth is form 0 to 200
Commit failed.
```

Example

- Set the maximum bandwidth for a CPU queue to 200 pps.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler3 max-bandwidth-pps 200
admin@XorPlus# commit
```

set class-of-service scheduler min-bandwidth-pps

The **set class-of-service scheduler min-bandwidth-pps** command sets the minimum bandwidth for a CPU queue.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **min-bandwidth-pps** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
min-bandwidth-pps <*value*>	Specifies the minimum bandwidth for a CPU queue. The value is an integer.

Usage Guidelines

The total value of min-bandwidth-pps of all activated queues should be less than the CPU-affordable PPS depending on different platforms, which should be the maximum PPS threshold to the CPU.

Example

- Set the minimum bandwidth for a CPU queue to 20 pps.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler4 min-bandwidth-pps 20
admin@XorPlus# commit
```

set class-of-service scheduler-profile copp-profile forwarding-classs scheduler

The **set class-of-service scheduler-profile copp-profile forwarding-classs scheduler** command creates a CoPP scheduler profile.

Command Syntax

set class-of-service scheduler-profile copp-profile forwarding-classs <*forwarding-class-name*> **scheduler** <*scheduler-name*>

Parameter

Parameter	Description
forwarding-class <*forwarding-class-name* >	Specifies forwarding class, the value is a string, spaces are not allowed.
scheduler <*copp-scheduler -name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.

Usage Guidelines

The scheduler profile creates a mapping between the forwarding class and the copp scheduler, which define a scheduling strategy for the CPU queue and the queue shaping policy.

Example

- Create a CoPP scheduler profile.

```
admin@XorPlus# set class-of-service scheduler-profile copp-profile forwarding-classs copp-class3 scheduler copp-sch
admin@XorPlus# commit
```

set class-of-service scheduler weight (CoPP)

The **set class-of-service scheduler weight** command sets scheduler weight for a CPU queue, CoPP uses WRR algorithm for queue scheduling.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **weight** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
weight <*value*>	Specifies scheduler weight. The value is an integer that ranges from 1 to 32, refer to Table 2 for default value of the scheduler weight.

Usage Guidelines

Weighted Round Robin (WRR) algorithm ensures that packets in all the queues are scheduled in turn.

When using WRR scheduling, it is necessary to set weight for each queue. The device schedules queues in turn according to their weight value. A bigger weight value indicates a higher priority.

Note:

It is NOT recommended to use the weight value for CPU queue scheduling due to hardware restrictions.

Example

- Set scheduler weight for copp-scheduler3 to 30.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler3 weight 30
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-address-ipv4

The **set firewall filter copp sequence from destination-address-ipv4** command configures a firewall filter rule based on the destination IPv4 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-address-ipv4 <*ipv4-address*>	Specifies destination IP, it could be an IPv4 subnet. For example, 10.1.1.0/24.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-address-ipv4** command to configure a firewall filter rule based on the destination IPv4 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination IPv4 address of 10.1.1.0/24.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-address-ipv4 10.1.1.0/24
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-address-ipv6

The **set firewall filter copp sequence from destination-address-ipv6** command configures a firewall filter rule based on the destination IPv6 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-address-ipv6 <*ipv6-address*>	Specifies destination IPv6, it could be an IPv6 subnet. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers. For example, 2001::1/32.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-address-ipv6** command to configure a firewall filter rule based on the destination IPv6 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination IPv6 address of 2001::1/128.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-address-ipv6 2001::1/128
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-mac-address

The **set firewall filter copp sequence from destination-mac-address** command configures a firewall filter rule based on the destination MAC address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-mac-address** <*mac-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-mac-address <*mac-address*>	Specifies the destination MAC address. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-mac-address** command to configure a firewall filter rule based on the destination MAC address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination MAC address of 00:50:ba:27:be:d2.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-mac-address 00:50:ba:27:be:d2
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-port

The **set firewall filter copp sequence from destination-port** command configures a firewall filter rule based on the destination port for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-port** <*port-number*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-port <*port-number*>	Specifies the destination port number or port number range, for example, 5000 or 7000..7050.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-port** command to configure a firewall filter rule based on the destination port for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the destination port of 3222.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-port 3222
admin@XorPlus# commit
```

set firewall filter copp sequence from ether-type

The **set firewall filter copp sequence from ether-type** command configures a firewall filter rule based on the Ether-Type values for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from ether-type** <*ether-type*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
ether-type <*ether-type*>	Specifies an Ether-Type value. The value is an integer in decimal format that ranges from 1501 to 65535.

Usage Guidelines

You can run the **set firewall filter copp sequence from ether-type** command to configure a firewall filter rule based on the Ether-Type for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the Ether-Type value 34525.

```
admin@XorPlus# set firewall filter copp sequence 51 from ether-type 34525
admin@XorPlus# commit
```

set firewall filter copp sequence from protocol

The **set firewall filter copp sequence from protocol** command configures a firewall filter rule based on the protocol type for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from protocol** [**icmp | igmp | ip | ospf | others** <*protocol-number*> | **udp | tcp**]

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
protocol [icmp | igmp | ip | ospf | others <*protocol-number*> **| udp | tcp]**	Specifies a protocol name or a protocol number. Protocol name could be **icmp, igmp, ip, ospf, udp** or **tcp**. Protocol number is an integer that ranges from 0 to 255. For example, 8 for EGP, 9 for IGP, 47 for GRE, 88 for EIGRP, 103 for PIM, and 112 for VRRP.

Usage Guidelines

You can run the **set firewall filter copp sequence from protocol** command to configure a firewall filter rule based on the protocol type for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

BPDU, LLDP, LACP and ARP cannot be classified through the protocol field, as they are not an IP protocol. You can classify these protocol packets in other matching fields, such as destination-mac-address, destination-port and ether-type.

NOTE:

set firewall filter copp sequence from protocol icmp and **set firewall filter copp sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter copp sequence from protocol others** command with the protocol number.

Example

• Configure a firewall filter rule based on ICMP protocol.

```
admin@XorPlus# set firewall filter copp sequence 51 from icmp
admin@XorPlus# commit
```

set firewall filter copp sequence from source-address-ipv4

The **set firewall filter copp sequence from source-address-ipv4** command configures a firewall filter rule based on the source IPv4 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-address-ipv4 <*ipv4-address*>	Specifies source IP, it could be an IPv4 subnet. For example, 10.1.1.0/24.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-address-ipv4** command to configure a firewall filter rule based on the source IPv4 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the source IPv4 address of 10.1.1.0/24.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-address-ipv4 10.1.1.0/24
admin@XorPlus# commit
```

set firewall filter copp sequence from source-address-ipv6

The **set firewall filter copp sequence from source-address-ipv6** command configures a firewall filter rule based on the source IPv6 address for traffic classification.

Command Syntax

set firewall filter copp sequence *<number>* **from source-address-ipv6** *<ipv6-address>*

Parameter

Parameter	Description
sequence *<number>*	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-address-ipv6 *<ipv6-address>*	Specifies source IPv6, it could be an IPv6 subnet. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers. For example, 2001::1/128.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-address-ipv6** command to configure a firewall filter rule based on the source IPv6 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source IPv6 address of 2001:a100::1/128.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-address-ipv6 2001:a100::1/128
admin@XorPlus# commit
```

set firewall filter copp sequence from source-mac-address

The **set firewall filter copp sequence from source-mac-address** command configures a firewall filter rule based on the source MAC address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-mac-address** <*mac-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-mac-address <*mac-address*>	Specifies the source MAC address. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-mac-address** command to configure a firewall filter rule based on the source MAC address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source MAC address of 11:50:ba:27:be:d2.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-mac-address 11:50:ba:27:be:d2
admin@XorPlus# commit
```

set firewall filter copp sequence from source-port

The **set firewall filter copp sequence from source-port** command configures a firewall filter rule based on the source port for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-port** <*port-number*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-port <*port-number*>	Specifies the source port number or port number range, for example, 5000 or 7000..7050.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-port** command to configure a firewall filter rule based on the source port for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source port of 3222.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-port 3222
admin@XorPlus# commit
```

set firewall filter copp sequence from vlan

The **set firewall filter copp sequence from vlan** command configures a firewall filter rule based on the VLAN ID for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from vlan** <*vlan-id*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

You can run the **set firewall filter copp sequence from vlan** command to configure a firewall filter rule based on the vlan ID for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the VLAN 2.

```
admin@XorPlus# set firewall filter copp sequence 51 from vlan 2
admin@XorPlus# commit
```

set firewall filter copp sequence then forwarding-class

The **set firewall filter copp sequence then forwarding-class** command sets forwarding class of CoPP policy.

Command Syntax

set firewall filter copp sequence <*number*> **then forwarding-class** <*forwarding-class-name*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
forwarding-class <*forwarding-class-name* >	Specifies forwarding class name, the value is a string type, spaces are not allowed.

Usage Guidelines

After configuring a forwarding class, user could use the **set class-of-service forwarding-class local-priority** command to set mapping between forwarding class and local priority.

Example

• Set sequence number 51 to forwarding class copp-class7.

```
admin@XorPlus# set firewall filter copp sequence 51 then forwarding-class copp-class7
admin@XorPlus# commit
```

set firewall filter copp sequence then dscp

The **set firewall filter copp sequence then dscp** command remarks the DSCP priority in packets for COPP.

Command Syntax

set firewall filter copp sequence <*number*> **then dscp** <*dscp-value*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
dscp <*dscp-value*>	Specifies a value to remark the DSCP priority in packets. The value is an integer in the range of 0 to 63.

Usage Guidelines

To provide differentiated services based on the DSCP priority, run this command to configure the device to remark the DSCP priority in IP packets in a traffic behavior. The DSCP remark function is enabled only when a remarked DSCP priority is set by the user.

Whether the DSCP remark is applied to the inbound or outbound direction on the CPU interface, the device still processes outgoing packets based on the original priority value in the packets, but all the downstream Layer 3 devices processes the packets based on the remarked priority.

Example

- Remark the DSCP priority in packets to 20 for COPP.

```
admin@Xorplus# set firewall filter copp sequence 51 then dscp 20
```

run show copp bandwidth

The **run show copp bandwidth** command displays the CoPP policy information of forwarding class, including bandwidth information, scheduling information and local priority mapping.

Command Syntax

run show copp bandwidth

Parameter

None.

Example

• Show CoPP policy information of forwarding class.

```
admin@Xorplus# run show copp bandwidth
Forwarding Class  Min-Bandwidth Max-Bandwidth Weight Local-Priority Schedule-Mode
default-class        0            80           8      0              WRR
pim-class            0            80           16     8              WRR
igmp-class           0            80           16     9              WRR
vrrp-class           0            80           16     10             WRR
dhcp-class           0            80           16     11             WRR
rip-class            0            80           16     12             WRR
ospf-class           0            80           16     13             WRR
bgp-class            0            80           16     14             WRR
mlag-mac-sync-class  0            80           16     15             WRR
mlag-class           0            80           16     16             WRR
bfd-class            0            80           16     17             WRR
arp-class            20           80           32     18             WRR
arp-class            20           80           32     19             WRR
lldp-class           20           80           32     20             WRR
lacp-class           20           80           32     21             WRR
bpdu-class           20           80           32     22             WRR
management-class     20           80           12     23             WRR
mvrp-class           100          500          32     24             WRR
erps-class           100          500          32     25             WRR
ripng-class          0            500          16     26             WRR
loopback-detection-class   100    500          32     27             WRR
isis-class           0            80           16     13             WRR
```

run show copp statistics

The **run show copp statistics** command displays the statistics information of the forwarding class, including input and dropped packets and rate.

Command Syntax

run show copp statistics [**active** | **forwarding-class** <*forwarding-class-name*>]

Parameter

Parameter	Description
active	Optional. Specifies state of the forwarding class. With this parameter, only shows the statistics information of the active forwarding class.
forwarding-class <*forwarding-class-name*>	Optional. Specifies forwarding class name, the value is a string type, spaces are not allowed.

Example

• Show the statistics information of the forwarding class.

```
admin@Xorplus# run show copp statistics
All Copp Traffic statistics:
Input rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Input Octets..............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets..............................0
Drop Octets...............................0

default-class Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Input Octets..............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets..............................0
Drop Octets...............................0

pim-class Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Input Octets..............................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets..............................0
Drop Octets...............................0

......
```

run show interface stm

The **run show interface stm** command displays the total STM resources that are available and how many STM entries are in use.

Note:

It is allowed to configure the firewall filter rule only when there are available STM resources.

Command Syntax

run show interface stm

Parameter

None.

Example

• Show the information of STM resources.

```
admin@Xorplus# run show interface stm
Total stm resource:
  Share-mode: 5
  number of host routes: 32768
  number of mac unicast addresses: 32768
  number of firewall ingress tables: 896
  number of firewall egress tables: 510
  number of IPv4 unicast routes: 5000
  number of IPv6 unicast routes: 500
Stm resource in use:
  number of firewall ingress tables: 2
  number of firewall egress tables: 29
```

The item **number of firewall egress tables** is used for describing STM resources of CoPP. By default, the value of **number of firewall egress tables** in **Stm resource in use:** is 21 as have been used by the default CoPP configurations.

run clear copp statistics

The **run clear copp statistics** command clears the past statistics information of CoPP policy.

Command Syntax

run clear copp statistics

Parameter

None.

Usage Guidelines

If you want to obtain the latest statistics information of CoPP policy, use this command to clear the past statistics information, When new packets coming, new statistics information is generated.

Example

• Clear the past statistics information of CoPP policy.

```
admin@Xorplus# run clear copp statistics
admin@Xorplus# commit
```

set class-of-service forwarding-class local-priority (CoPP)

The **set class-of-service forwarding-class local-priority** command sets mapping between forwarding class and local priority, the switch will then send different types of packets to the specific CPU queue.

Command Syntax

set class-of-service forwarding-class <*forwarding-class-name*> **local-priority** <*int*>

Parameter

Parameter	Description
forwarding-class <*forwarding-class-name*>	Specifies forwarding class, the value is a string, spaces are not allowed.
local-priority <*int*>	Specifies local priority corresponding to the CPU queue. The value is an integer that ranges from 0 to 23.

Example

• Set forwarding class copp-class3 to CPU queue 20.

```
admin@XorPlus# set class-of-service forwarding-class copp-class3 local priority 20
admin@XorPlus# commit
```

run show filter copp

The **run show filter copp** command displays the configuration information of all CoPP policies, both pre-defined and user-defined, and match counter.

Command Syntax

run show filter copp [**sequence <***number***>**]

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.

Example

• Show the configuration information of all CoPP policies, both pre-defined and user-defined, and match counter.

```
admin@Xorplus# run show filter copp
Filter:copp
      Description:
      Sequence: 10
          Description:
          match counter:  0 packets
          match-condition:
              protocol:                bpdu
          action: forward
          forwarding_class: bpdu-class
          ......
      Sequence: 81
          Description:
          match counter:  0 packets
          match-condition:
              destination-port:        23..23
              protocol:                tcp
          action: forward
          forwarding_class: copp-class3
          ......
      Input interface: inbound-control-plane
```

Buffer Management Commands

- set interface ethernet-switching-options buffer egress-queue shared-ratio
- set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
- run show interface egress-buffer
- run show interface gigabit-ethernet egress-queues

set interface ethernet-switching-options buffer egress-queue shared-ratio

The **set interface ethernet-switching-options buffer shared-ratio** command sets the dynamic threshold ratio of the available shared space.

Command Syntax

set interface ethernet-switching-options buffer egress-queue <*queue-index*> **shared-ratio** <*ratio-value*>

Parameter

Parameter	Description
egress-queue <*queue-index*>	Specifies the interface queue. The value is an integer that ranges from 0 to 7. NOTE: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
shared-ratio <*ratio-value*>	Specifies the value of the dynamic threshold ratio of the available shared space. The value is an integer that ranges from 0 to 100, indicating 1% to 100%. The default value is 33.

Usage Guidelines

The dynamic mode of both multicast (must enable dynamic threshold) and unicast queues can configure the max dynamic threshold ratio. The threshold is still dynamically adjusted until reaching the max ratio configured.

For the maximum shared-area ratio for a queue, the percentage values 0 to 100 are divided into 10 rages. The table below shows the effective values that correspond to the configured values of ratio-value.

> **NOTE:**
>
> Currently, multicast queue just support eight (1~67) effective ratio value on all platforms.

Example

- Set the dynamic threshold ratio of the available shared space to 40%.

```
admin@Xorplus# set interface ethernet-switching-options buffer egress-queue 0 shared-ratio 40
admin@Xorplus# commit
```

set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared

The **set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared** command is used to enable or disable the dynamic mode of buffer management of the queue.

Command Syntax

set interface ethernet-switching-options buffer egress-queue <*queue-index*> **mc-queue-dynamic-shared** <**true** | **false**>

Parameter

Parameter	Description
egress-queue <*queue-index*>	Specifies the interface queue. The value is an integer that ranges from 0 to 7. **NOTE:** On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
mc-queue-dynamic-shared <**true**	**false**>	Enable or disable the dynamic mode of buffer management of the queue. The value could be **true** or **false**. • **true**: enable the dynamic mode of buffer management of the queue. • **false**: disable the dynamic mode of buffer management of the queue. By default dynamic mode of buffer management is disabled.

Usage Guidelines

1. Multicast queue

- static mode: This is the default configuration

The value of the static threshold is configured for the multicast queue in the shared space. This avoids the scenario where the port enabled flow control or PFC affects the forwarding of other ports. But the disadvantage is less efficient use of memory.

- dynamic mode: Need to configure

The memory threshold is adjusted dynamically according to the available shared memory in this mode. The thresholds value will dynamically decrease when the available shared memory decreases. The thresholds will rise up when the available shared memory rises up.

2. Unicast queue

- dynamic mode

Dynamic threshold is the default mode for the unicast queue, and it can't configure static threshold.

Example

- Enable or disable the dynamic mode of buffer management of queue 0.

```
admin@Xorplus# set interface ethernet-switching-options buffer egress-queue 0 mc-queue-dynamic-shared true
admin@Xorplus# commit
```

run show interface egress-buffer

The **run show interface egress-buffer** command displays the configuration information for the buffer management.

Command Syntax

run show interface egress-buffer

Parameter

None.

Example

- Display the configuration information for the buffer management.

```
admin@Xorplus# run show interface egress-buffer
Queue UC-Enabled UC-Shared-Ratio MC-Enabled MC-Shared-Ratio
0     true       33              false      --
1     true       33              false      --
2     true       33              false      --
3     true       33              false      --
4     true       33              false      --
5     true       33              false      --
6     true       33              false      --
7     true       33              false      --
```

run show interface gigabit-ethernet egress-queues

The **run show interface gigabit-ethernet egress-queues** command displays the traffic statistics on an outbound interface queue.

Command Syntax

run show interface gigabit-ethernet <*interface-name*> **egress-queues** <*queue-index*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of the physical interface. The value is a string.
egress-queue <*queue-index*>	Optional. Specifies the interface queue. The value is an integer that ranges from 0 to 7.

Example

- Display the traffic statistics on an outbound interface queue.

```
admin@Xorplus# run show interface gigabit-ethernet ge-1/1/20 egress-queues 1
OutPackets   :0
OutPacketsRate:0
OutBytes      :0
OutBytesRate  :0
DropPackets   :0
DropBytes    :0
UCqueuedBytes:0
MCqueuedBytes:0
UCDepth      :202730
MCDepth      :55328
```

Table 1 Description of the run show gigabit-ethernet egress-queues command output

Item	**Description**
OutPackets	Number of packets sent by an interface queue.
OutPacketsRate	Rate of packets sent by an interface queue.
OutBytes	Number of bytes sent by an interface queue.
OutBytesRate	Rate of bytes sent by an interface queue.
DropPackets	Number of packets dropped by an interface queue.
DropBytes	Number of bytes sent by an interface queue.

UCqueuedBytes	Number of unicast bytes buffered by an interface queue.
MCqueuedBytes	Number of multicast bytes buffered by an interface queue.
UCDepth	The total memory space of each queue for unicast bytes.
MCDepth	The total memory space of each queue for multicast bytes.

Interface-based Rate Limiting Commands

- set interface gigabit-ethernet rate-limiting ingress kilobits
- set interface gigabit-ethernet rate-limiting ingress ratio
- set interface gigabit-ethernet rate-limiting ingress burst
- set interface gigabit-ethernet rate-limiting egress kilobits
- set interface gigabit-ethernet rate-limiting egress ratio
- set interface gigabit-ethernet rate-limiting egress burst

set interface gigabit-ethernet rate-limiting ingress kilobits

The **set interface gigabit-ethernet rate-limiting ingress kilobits** command sets a rate limit value in kbit/s on a port for the ingress traffic.

NOTE:

- In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
- Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting ingress kilobits** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
kilobits *<value>*	Specifies the rate limit value in kbits/s. The value is an integer that ranges from 0 to 100000000. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 1000 kbit/s on port ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress kilobits 1000
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting ingress ratio

The **set interface gigabit-ethernet rate-limiting ingress ratio** command sets a rate limit value on a port for the ingress traffic in percentage.

NOTE:

- In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
- Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting ingress ratio** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
ratio *<value>*	Specifies the rate limit value in percentage of the interface rate. The value is an integer that ranges from 0 to 100. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 10% of the interface rate on ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress ratio 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting ingress burst

The **set interface gigabit-ethernet rate-limiting ingress burst** command sets a burst limit value on a port for the ingress traffic.

> **NOTE**:
>
> Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting ingress burst** *<burst-size>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
burst *<burst-size>*	Specifies the burst size in kbit, which is the maximum volume of burst traffic that can pass through an interface. The value is an integer from 1 to the value of interface rate. When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** *<interface-name>* **rate-limiting ingress kilobits** *<value>* or **set interface gigabit-ethernet** *<interface-name>* **rate-limiting ingress ratio** *<value>* command.

Example

- Set the burst size value to 10 kbit on port ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress burst 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress kilobits

The **set interface gigabit-ethernet rate-limiting egress kilobits** command sets a rate limit value in kbit/s on a port for the egress traffic.

> **NOTE**:
>
> In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting egress kilobits** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
kilobits *<value>*	Specifies the rate limit value in kbits/s. The value is an integer that ranges from 0 to 100000000. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 1000 kbit/s on port ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress kilobits 1000
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress ratio

The **set interface gigabit-ethernet rate-limiting egress ratio** command sets a rate limit value on a port for the egress traffic in percentage.

> **NOTE**:
>
> In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress ratio** <*value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value is a string.
ratio <*value*>	Specifies the rate limit value in percentage of the interface rate. The value is an integer that ranges from 0 to 100. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 10% of the interface rate on ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress ratio 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress burst

The **set interface gigabit-ethernet rate-limiting egress burst** command sets a burst limit value on a port for the egress traffic.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress burst** <*burst-size*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value is a string.
burst <*burst-size*>	Specifies the burst size in kbit, which is the maximum volume of burst traffic that can pass through an interface. The value is an integer from 1 to the value of interface rate. When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress kilobits** <*value*> or **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress ratio** <*value*> command.

Example

- Set the burst size value to 10 kbit on port ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress burst 10
admin@Xorplus# commit
```

ACL-based Traffic Policer Commands

- set firewall policer if-exceeding count-mode
- set firewall policer if-exceeding rate-limit
- set firewall policer if-exceeding burst-limit
- set firewall filter sequence then policer
- set firewall policer if-exceeding action discard
- run show policer

set firewall policer if-exceeding count-mode

The **set firewall policer if-exceeding count-mode** command configures the data rate units for the rate-limit and burst-limit of a policer. The value could be **packet** or **kbit**.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding count-mode** <*count-mode*>

Parameter

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
count-mode <*count-mode*>	Specifies the count mode for the rate-limit and burst-limit of a policer. The value could be **packet** or **kbit**. • **packet**: packet per second. • **kbit**: kbit per second. By default, the count mode is **packet**.

Usage Guidelines

When the count mode is **packet**, the range of rate-limit and burst-limit is from 1 to 1000 pps.

When the count mode is **kbit**, the range of rate-limit is from 0 to 100000000 kbit/s, and burst-limit is from 0 to 100000000 kbit.

Example

- Configure the count mode for the rate-limit and burst-limit the policer as **kbit** and use **run show policer** to check the configuration.

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode kbit
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
-----------  ----------   ----------    ----------   ----------
p1        5000       0        kbit      discard
```

set firewall policer if-exceeding rate-limit

The **set firewall policer if-exceeding rate-limit** command configures the rate limit value for a policer.

> **NOTE:**
> It is NOT recommended to use the rate limit value for CPU queue due to hardware restrictions.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding rate-limit** <*value*>

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
rate-limit <*value*>	Specifies the rate limit value of a policer. The data rate unit is **set by set firewall policer if-exceeding count-mode** command. • When the count mode is **packet**, the range of rate-limit is from 1 to 1000 pps. • When the count mode is **kbit**, the range of rate-limit is from 0 to 100000000 kbit/s.

Example

- The following example configures rate limiting for the *p1* policer to 100 pps (packets per second):

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode packet
admin@Xorplus# set firewall policer p1 if-exceeding rate-limit 100
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
------------   ----------   ----------    ----------   ----------
p1        100       0         packet      discard
```

set firewall policer if-exceeding burst-limit

The **set firewall policer if-exceeding burst-limit** command configures the burst limit value for a policer.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding burst-limit** <*value*>

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
burst-limit <*value*>	Specifies the burst limit value of a policer. The data rate unit is **set by set firewall policer if-exceeding count-mode** command. • When the count mode is **packet**, the range of burst-limit is from 0 to 1000 pps. • When the count mode is **kbit**, the range of burst-limit is from 0 to 100000000 kbit.

Example

- The following example configures burst limiting for the *p1* policer to 500 pps (packets per second).

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode packet
admin@Xorplus# set firewall policer p1 if-exceeding burst-limit 500
admin@Xorplus# run show policer
Policer         rate limit   burst limit   count mode  action
------------   ----------  ----------    ----------   ----------
p1              100          500           packet      discard
```

set firewall filter sequence then policer

The **set firewall filter sequence then policer** command configures the policer for packets matching a filter sequence.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **then policer** <*policer-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
policer <*policer-name*>	Specifies the policer name. The value is a string.

Example

- This example configures sequence 1 of the *MyFilter* filter to match packets with source address 192.168.1.1 and the *MyPolicer* policer to be applied to packets matching the *MyFilter* filter:

```
admin@Switch# set firewall filter MyFilter sequence 1 from source-address-ipv4  192.168.1.1/32
admin@Switch# set firewall filter MyFilter sequence 1 then policer MyPolicer
```

set firewall policer if-exceeding action discard

The **set firewall policer if-exceeding action discard** command configures the action to drop the packets for a policer.

Command Syntax

set firewall policer <*policer-name*> **then action discard**

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.

Usage Guidelines

When the user configures the rate limit or burst limit of an ACL-based traffic policer, the interface then drops the packets whose rate exceeds the rate limit value so that the traffic rate is limited within a proper range. The default action is discard if not configured.

Example

- Configure the action to drop the packets for a traffic policer.

```
admin@Xorplus# set firewall policer MyPolicer if-exceeding count-mode kbit
admin@Xorplus# set firewall policer MyPolicer if-exceeding rate-limit 5000
admin@Xorplus# set firewall policer p1 then action discard
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
------------   ----------   ----------    ----------    ----------
p1        5000         0        kbit       discard
```

run show policer

The **run show policer** command displays the policer configuration information.

Command Syntax

run show policer

Parameter

None.

Example

- Run **run show policer** command to view the policer configuration information.

```
admin@Xorplus# run show policer
policer     rate limit   burst limit   count mode   action
------------------------------------------------------------------------
 p1        5000          0          kbit      discard
```

PFC Commands

- set class-of-service pfc-profile code-point drop
- set class-of-service interface pfc-profile
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset
- set interface ethernet-switching-options buffer service-pool threshold
- set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom
- set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio
- set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold
- set class-of-service pfc-watchdog granularity
- set class-of-service pfc-watchdog restore-action
- set class-of-service pfc-watchdog code-point detect-interval
- set class-of-service pfc-watchdog code-point restore-interval
- set class-of-service interface pfc-watchdog code-point enable
- set class-of-service pfc-watchdog threshold period
- set class-of-service pfc-watchdog threshold count
- set class-of-service interface pfc-watchdog restore-mode
- run clear class-of-service interface pfc-watchdog auto
- run clear class-of-service interface pfc-watchdog manual
- run show pfc-watchdog stats
- run show pfc-watchdog config
- run show interface gigabit-ethernet ingress-buffer
- run show interface gigabit-ethernet egress-buffer
- set class-of-service interface pfc-uplink-group
- set class-of-service pfc-uplink-group original-dscp to-code-point
- set class-of-service pfc-uplink-group original-dscp dscp

set class-of-service pfc-profile code-point drop

The full name of pfc is priority flow control. This command defines pfc works on the specified code point.

Note: Lag interface doesn't support pfc, but it supports flow control now. If lag interface has enabled flow control, and its member port has enabled pfc, pfc is valid and flow control is invalid on this member port because pfc has higher priority than flow control.

Command Syntax

set class-of–service pfc-profile <*profile-name*> **code-point** <*code-point*> **drop** <*boolean*>
delete class-of–service pfc-profile <*profile-name*> **code-point** <*code-point*> **drop**

Parameter

- <*profile-name*> Profile name, string type.
- <*code-point*> 0~7 value, only match ieee802.1p field.
- <*boolean*> Value is true or false. Default value is false. If value is false, priority flow control function is enabled on this code point. Otherwise, priority flow control function is disabled on this code point.

Example

• This example creates a pfc profile without any code point configuration. The default is that pfc is enabled on 0~7 code point.

```
admin@XorPlus# set class-of-service pfc-profile pfc1
admin@XorPlus# set class-of-service interface ge-1/1/1 pfc-profile pfc1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
802.1P         Priority Flow Control
-----------    --------------------
0              true
1              true
2              true
3              true
4              true
5              true
6              true
7              true
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule           Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
```

```
7               SP,0kbps
```

• This example creates a pfc profile with code point 2 drop true.

```
admin@XorPlus# set class-of-service pfc-profile pfc2 code-point 2 drop true
admin@XorPlus# set class-of-service pfc-profile pfc2 code-point 4 drop true
admin@XorPlus# set class-of-service interface ge-1/1/2 pfc-profile pfc2
admin@XorPlus# commit
Commit OK.
Save done.

admin@XorPlus# run show class-of-service interface ge-1/1/2
Interface : ge-1/1/2
802.1P         Priority Flow Control
-----------    --------------------
0              true
1              true
2              false
3              true
4              false
5              true
6              true
7              true
trust mode : ieee-802.1
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule           Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps

```

set class-of-service interface pfc-profile

The full name of pfc is priority flow control. This command define pfc is applied in a specified port. Pfc acts on packets entering the port, similar to flow control. But flow control only works on the port. It can't work on the code point.

When flow control has been configured on the port, configure pfc. Because pfc has higher priority than flow control, flow control will become invalid on the port.

Command Syntax

set class-of–service interface *<port>* **pfc-profile** *<profile-name>*

delete class-of–service interface *<port>* **pfc-profile**

Parameter

- *<port>* Physical interface.
- *<profile-name>* pfc profile name, which has been defined in class-of-service pfc-profile in advance.

Example

This example of a pfc profile applied in a port.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 pfc-profile pfc1
admin@XorPlus# commit
Commit OK.
Save done.
```

set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed

The **set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed** command can be used to set the upper threshold of guaranteed buffer for a PFC queue on the ingress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer ingress-queue guaranteed** command deletes the configuration. configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **guaranteed** <*value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**ingress-queue** <*queue-id*>] [**guaranteed**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
guaranteed <*value*>	Specifies the upper threshold of guaranteed buffer for a PFC queue on the ingress interface. When the guaranteed buffer threshold is reached, the packets will occupy the shared service pool. The value is an integer that ranges from 1 to 65535. Unit: cell. **Note**: The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the upper threshold of guaranteed buffer for PFC queue 3 on the ingress interface xe-1/1/3 as 2400 cells.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer ingress-queue 3
guaranteed 2400
```

```
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio

The **set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio** can be used to set the dynamic threshold of shared buffer for a PFC queue on the ingress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer ingress-queue shared-ratio** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **shared-ratio** <*ratio-value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**ingress-queue** <*queue-id*>] [**shared-ratio**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
shared-ratio <*ratio-value*>	Specifies the ratio of the shared buffer remaining space for a PFC queue on the ingress interface. When the occupied buffer space exceeds the specified threshold (a dynamic value, which equals to *ratio* multiply *remaining space*), the Pause frame will be generated and sent to the egress interface. The value is an integer that ranges from 0 to 100. Unit: %.

Example

- Set the ratio of the shared buffer remaining space for PFC queue 3 on the ingress interface xe-1/1/3 as 30%.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer ingress-queue 3 shared-ratio 30%
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold

The **set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold** can be used to set the static threshold of shared buffer for a PFC queue on the ingress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer ingress-queue threshold** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **threshold** <*value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**ingress-queue**<*queue-id*>] [**threshold**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
threshold <*value*>	Specifies the static threshold of shared buffer for a PFC queue on the ingress interface. When the occupied buffer space exceeds the specified threshold, the Pause frame will be generated and sent to the egress interface. The value is an integer that ranges from 1 to 65535. Unit: cell. **Note**: The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the static threshold of shared buffer for PFC queue 3 on the ingress interface xe-1/1/3 as 2400.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer ingress-queue 3
threshold 2400
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset

The **set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset** can be used to set the offset value of shared buffer for a PFC queue on the ingress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer ingress-queue reset-offset** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **reset-offset** <*value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**ingress-queue** <*queue-id*>] [**reset-offset**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
reset-offset <*value*>	Set the offset value of shared buffer for a PFC queue on the ingress interface. The Pause frames will stop being generated when the occupied space is reduced to a certain level (the upper threshold minus the offset value). The value is an integer that ranges from 1 to 65535. Unit: cell. **Notes**: • The value should be lower than the shared threshold. • The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the offset value of shared buffer for PFC queue 3 on the ingress interface xe-1/1/3 as 2400.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer ingress-queue 3 reset-offset 2400
admin@PICOS# commit
```

set interface ethernet-switching-options buffer service-pool threshold

The **set interface ethernet-switching-options buffer service-pool threshold** can be used to set the global threshold of shared buffer for all ingress interfaces.

The **delete interface ethernet-switching-options buffer service-pool threshold** command deletes the configuration.

Command Syntax

set interface ethernet-switching-options buffer service-pool 0 threshold <*value*>

delete interface ethernet-switching-options [**buffer**] [**service-pool 0**] [**threshold**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
service-pool 0	Specifies the service pool of shared buffer as 0.
threshold <*value*>	Specifies the global threshold of shared buffer for all ingress interfaces. When the occupied space of an interface exceeds the specified threshold, the packets will be saved in the headroom buffer. The value is an integer that ranges from 1 to 120000. Unit: cell. **Note**: The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the global threshold of shared buffer for all ingress interfaces as 100000.

```
admin@PICOS# set interface ethernet-switching-options buffer service-pool 0 threshold 100000
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom

The **set interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom** command can be used to set the upper threshold of headroom buffer for a PFC queue on the ingress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer ingress-queue headroom** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer ingress-queue** <*queue-id*> **headroom** <*value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**ingress-queue** <*queue-id*>] [**headroom** <*value*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the ingress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an ingress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
headroom <*value*>	Specifies the upper threshold of headroom buffer for a PFC queue on the ingress interface. When the headroom buffer threshold is reached, the received packets will be dropped. The value is an integer that ranges from 1 to 65535. Unit: cell. **Note**: The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the upper threshold of headroom buffer for PFC queue 3 on the ingress interface xe-1/1/3 as 2400 cells.

```
admin@PICOS# set interface gigabit-ethernet ge-1/1/3 ethernet-switching-options buffer ingress-queue 3 headroom
2400
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio

The **set interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio** can be used to set the dynamic threshold of shared buffer for a PFC queue on the egress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer egress-queue shared-ratio** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer egress-queue** <*queue-id*> **shared-ratio** <*ratio-value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**egress-queue** <*queue-id*>] [**shared-ratio**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the egress direction of the downstream switch.
ingress-queue <*queue-id*>	Specifies the queue number of an egress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
shared-ratio <*ratio-value*>	Specifies the ratio of shared buffer remaining space for a PFC queue on the egress interface. When the occupied buffer space exceeds the specified threshold (a dynamic value, which equals to *ratio* multiply *remaining space*), the packets will be saved in the headroom buffer. The value is an integer that ranges from 0 to 100. Unit: %.

Example

- Set the ratio of shared buffer remaining space for PFC queue 3 on the egress interface xe-1/1/3 as 30%.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer egress-queue 3 shared-ratio 30%
admin@PICOS# commit
```

set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold

The **set interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold** can be used to set the static threshold of shared buffer for a PFC queue on the egress interface.

The **delete interface gigabit-ethernet ethernet-switching-options buffer egress-queue threshold** command deletes the configuration.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **ethernet-switching-options buffer egress-queue** <*queue-id*> **threshold** <*value*>

delete interface gigabit-ethernet <*interface-name*> **ethernet-switching-options** [**buffer**] [**egress-queue**<*queue-id*>] [**threshold**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of a physical interface in the egress direction of the downstream switch.
egress-queue <*queue-id*>	Specifies the queue number of an egress interface. The value is an integer that ranges from 0 to 7. **Note**: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
threshold <*value*>	Specifies the static threshold of shared buffer for a PFC queue on the egress interface. When the occupied buffer space exceeds the specified threshold, the packets will be saved in the headroom buffer. The value is an integer that ranges from 1 to 65535. Unit: cell. **Note**: The values of cell are different on different platforms. The value is **256** bytes on Trident3-X5 and Trident3-X7 platforms, and is **254** bytes on the Tomahawk3 platform.

Example

- Set the static threshold of shared buffer for PFC queue 3 on the egress interface xe-1/1/3 as 2400.

```
admin@PICOS# set interface gigabit-ethernet xe-1/1/3 ethernet-switching-options buffer egress-queue 3 threshold
2400
```

```
admin@PICOS# commit
```

set class-of-service pfc-watchdog granularity

The **set class-of-service pfc-watchdog granularity** command configures the granularity of the PFC deadlock detection and restore timer.

The **delete class-of-service pfc-watchdog granularity** command restores the default configuration.

Command Syntax

set class-of-service pfc-watchdog granularity <**10** | **100**>

delete class-of-service pfc-watchdog granularity

Parameter

Parameter	Description
granularity <**10** | **100**>	Specifies the granularity of the PFC deadlock detection timer and restore timer. The value could be **10** or **100**, in milliseconds. The default value is 100 ms.

Usage Guidelines

Use this command to adjust the granularity of the PFC deadlock detection timer, thereby controlling the PFC deadlock detection time.

Example

- Configure the granularity of the PFC deadlock detection and restore timer to 10 ms.

```
admin@PICOS# set class-of-service pfc-watchdog granularity 10
admin@PICOS# commit
```

set class-of-service pfc-watchdog restore-action

The **set class-of-service pfc-watchdog restore-action** command configures the restore action after a deadlock is detected on the device.

The **delete class-of-service pfc-watchdog restore-action** command restores the default configuration.

Command Syntax

set class-of-service pfc-watchdog restore-action <**forward** | **drop**>

delete class-of-service pfc-watchdog restore-action

Parameter

Parameter	Description
restore-action <**forward** | **drop**>	Configures the restore action after a deadlock is detected on the device. The value could be **forward** or **drop**. • **forward**: forwards received data packets. • **drop**: drops received data packets. The default value is **forward**.

Usage Guidelines

During the PFC deadlock recovery process, the received PFC PAUSE frame will be ignored, and the internal scheduler will resume forwarding the traffic. It is also possible to configure the system to drop the traffic and restore the normal PFC flow control mechanism after the recovery timer.

Example

- Configure the restore action after a deadlock occurs on the device.

```
admin@PICOS# set class-of-service pfc-watchdog restore-action drop
admin@PICOS# commit
```

set class-of-service pfc-watchdog code-point detect-interval

The **set class-of-service pfc-watchdog code-point detect-interval** command configures the time interval of PFC deadlock detection. The value of detection time depends on the configured **granularity** and **detect-timer**, the value of detection time = **granularity** x **detect-interval**.

The **delete class-of-service pfc-watchdog code-point detect-interval** command restores the default configuration.

Command Syntax

For Trident3 platforms:

set class-of-service pfc-watchdog code-point <*cos*> **detect-interval** <*detect-interval*>

delete class-of-service pfc-watchdog code-point <*cos*> **detect-interval**

For Tomahawk3 platforms:

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **detect-interval** <*detect-interval*>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **detect-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
detect-interval <*detect-interval*>	Specifies the time interval of PFC deadlock detection. The value is an integer that ranges from 1 to 15. The default value is 15.

Usage Guidelines

After receiving the PFC Pause frame, the internal scheduler will stop forwarding the queue traffic of corresponding priority and start the timer to detect the PFC Pause frame received by the queue based on the set deadlock detection and granularity.
If the queue remains under flow control state within the configured PFC deadlock detection time, it is considered that a PFC deadlock has occurred and a PFC deadlock restore process is required.

Example

- Configure the time interval of PFC deadlock detection.

```
admin@PICOS# set class-of-service pfc-watchdog code-point 5 detect-interval 10
admin@PICOS# commit
```

set class-of-service pfc-watchdog code-point restore-interval

The **set class-of-service pfc-watchdog code-point restore-interval** command configures the restore time when PFC deadlock occurs. The value of restore time depends on the configured **granularity** and **restore-interval**, the restore time = **granularity** x **restore-interval**.

The **delete class-of-service pfc-watchdog code-point restore-interval** command restores the default configuration.

Command Syntax

For Trident3 platforms:

set class-of-service pfc-watchdog code-point <*cos*> **restore-interval** <*restore-interval*>

delete class-of-service pfc-watchdog code-point <*cos*> **restore-interval**

For Tomahawk3 platforms:

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **restore-interval** <*restore-interval*>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **restore-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
restore-interval <*restore-interval*>	Specifies the restore time when PFC deadlock occurs. The value is an integer that ranges from 1 to 15. The default value is 15.

Usage Guidelines

When a PFC deadlock has occurred and a PFC deadlock restore process is required. During the PFC deadlock recovery process, the PFC PAUSE frames received by the port will be ignored, and the internal scheduler will resume sending queue traffic of corresponding priority. It is also possible to choose to drop queue traffic of the corresponding priority and restore normal PFC flow control mechanism after the restore time.

Example

- Configure the restore time when PFC deadlock occurs.

```
admin@PICOS# set class-of-service pfc-watchdog code-point 5 restore-interval 10
admin@PICOS# commit
```

set class-of-service interface pfc-watchdog code-point enable

The **set class-of-service interface pfc-watchdog code-point enable** command enables PFC watchdog functionality.

The **delete class-of-service interface pfc-watchdog code-point enable** command restores the default configuration.

Command Syntax

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable** <**true** | **false**>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port. The default value is 100 ms.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
enable <**true**	**false**>	Enables or disables PFC watchdog functionality. The value could be **true** or **false**. • **true**: enables PFC watchdog functionality. • **false**: disables PFC watchdog functionality. By default, PFC watchdog is disabled.

Example

- Enable PFC watchdog functionality.

```
admin@PICOS# set class-of-service interface ge-1/1/1 pfc-watchdog code-point 5 enable true
admin@PICOS# commit
```

set class-of-service pfc-watchdog threshold period

The **set class-of-service pfc-watchdog threshold period** command configures the period for PFC deadlock occurrences. When PFC watchdog functionality is enabled and the restore mode for a port is set to automatic recovery, and the number of PFC deadlocks reaches the upper limit within the specified period, the PFC function on that port will be disabled. The command **set class-of-service pfc-watchdog threshold count** <*count*> can be used to configure the upper limit number of PFC deadlocks occurrences.

The **delete class-of-service pfc-watchdog threshold period** command deletes the configuration.

Command Syntax

set class-of-service pfc-watchdog threshold period <*time*>

delete class-of-service pfc-watchdog threshold period

Parameter

Parameter	Description
period <*time*>	Specifies the time period in seconds. The value is an integer ranging from 1 to 60. The default value is 20 seconds.

Usage Guidelines

When PFC watchdog functionality is enabled and the restore mode for a port is set to automatic recovery, the PFC watchdog continuously monitors the PFC activity on the port. If deadlocks repeatedly occur and the count exceeds the configured threshold within the specified time period, the system determines that the port is in an unstable state and will automatically disable the PFC feature to prevent further network disruption.

Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

This ensures that persistent deadlocks do not degrade network performance.

Example

- Configure the period for PFC deadlock occurrences.

```
admin@PICOS# set class-of-service pfc-watchdog threshold period 20
admin@PICOS# commit
```

set class-of-service pfc-watchdog threshold count

The **set class-of-service pfc-watchdog threshold count** command configures the maximum number of PFC deadlocks occurrences within a specified period. When PFC watchdog functionality is enabled and the restore mode for a port is set to automatic recovery, and the number of PFC deadlocks reaches the upper limit within the specified period, the PFC function on that port will be disabled. The command **set class-of-service pfc-watchdog threshold period** <*time*> can be used to configure the specified period.

The **delete class-of-service pfc-watchdog threshold count** command deletes the configuration.

Command Syntax

set class-of-service pfc-watchdog threshold count <*count*>

delete class-of-service pfc-watchdog threshold count

Parameter

Parameter	Description
count <*count*>	Specifies the maximum number of PFC deadlocks. The value is an integer ranging from 1 to 500. The default value is 30.

Usage Guidelines

When PFC watchdog functionality is enabled and the restore mode for a port is set to automatic recovery, the PFC watchdog continuously monitors the PFC activity on the port. If deadlocks repeatedly occur and the count exceeds the configured threshold within the specified time period, the system determines that the port is in an unstable state and will automatically disable the PFC feature to prevent further network disruption.

Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

This ensures that persistent deadlocks do not degrade network performance.

Example

- Configure the maximum number of PFC deadlocks occurrences within a specified period.

```
admin@PICOS# set class-of-service pfc-watchdog threshold count 15
admin@PICOS# commit
```

set class-of-service interface pfc-watchdog restore-mode

The **set class-of-service interface pfc-watchdog restore-mode** command configures the restore mode for a deadlocked port.

The **delete class-of-service interface pfc-watchdog restore-mode** command deletes the configuration.

Command Syntax

set class-of-service interface <*interface-name*> **pfc-watchdog restore-mode <manual | auto>**

delete class-of-service interface <*interface-name*> **pfc-watchdog restore-mode**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical port name where PFC watchdog can be enabled. The interface could be a physical port or a member port of a LAG port.
restore-mode <manual | auto>	Specifies the restore mode for a deadlocked port. The value could be **manual** or **auto**. • **manual**: Specifies the restore mode for a deadlocked port to **manual**. • **auto**: Specifies the restore mode for a deadlocked port to **auto**. The default value is **auto**.

Usage Guidelines

The system supports two different restore modes: **Manual** and **Auto**, representing different deadlock detection processes and different PFC deadlock recovery methods:

- **Auto**

When PFC watchdog functionality is enabled and the restore mode for a port is set to **Auto** recovery, the PFC watchdog continuously monitors the PFC activity on the port. If deadlocks repeatedly occur and the count exceeds the configured threshold within the specified time period, the system determines that the port is in an unstable state and will automatically disable the PFC feature to prevent further network disruption.

Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

- **Manual**

When PFC watchdog functionality is enabled and the restore mode for a port is set to **Manual** recovery, the PFC watchdog continuously monitors the PFC activity on the port, once a PFC deadlock occurs, the PFC function on that port will be automatically disabled.

Once PFC is disabled, the port will no longer use PFC to manage congestion until it is manually reset by using the following command:

run clear class-of-service interface <*interface-name*> **pfc-watchdog manual**

This ensures that persistent deadlocks do not degrade network performance.

Example

- Configure the restore mode to **manual** for port xe-1/1/1.

```
admin@PICOS# set class-of-service interface xe-1/1/1 pfc-watchdog restore-mode manual
admin@PICOS# commit
```

run clear class-of-service interface pfc-watchdog auto

The **run clear class-of-service interface pfc-watchdog auto** command re-enables the PFC watchdog function when the restore mode is set to *auto*.

Command Syntax

run clear class-of-service interface <*interface-name*> **pfc-watchdog auto**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical port name where PFC watchdog can be enabled. The interface could be a physical port or a member port of a LAG port.

Usage Guidelines

Before configuring this command, you need to execute the **set class-of-service interface** <*interface-name*> **pfc-watchdog restore-mode auto** command to set the PFC deadlock detection recovery mode to auto.

If deadlocks repeatedly occur and the count exceeds the configured threshold within the specified time period, the system will automatically disable the PFC function. Users need to manually execute this command to restore the PFC deadlock detection function. Restoring the PFC deadlock detection function will also allow the PFC function to continue operating.

Example

- Re-enable the PFC function when the restore mode is set to **auto**

```
admin@PICOS#run clear class-of-service interface xe-1/1/1 pfc-watchdog auto
```

run clear class-of-service interface pfc-watchdog manual

The **run clear class-of-service interface pfc-watchdog manual** command re-enables the PFC watchdog function when the restore mode is set to *manual*.

Command Syntax

run clear class-of-service interface <*interface-name*> **pfc-watchdog manual**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical port name where PFC watchdog can be enabled. The interface could be a physical port or a member port of a LAG port.

Usage Guidelines

Before configuring this command, you need to execute the **set class-of-service interface** <*interface-name*> **pfc-watchdog restore-mode manual** command to set the PFC deadlock detection recovery mode to manual.

PFC watchdog continuously monitors the PFC activity on the port, once a PFC deadlock occurs, the PFC function on that port will be automatically disabled. Users need to manually execute this command to restore the PFC deadlock detection function. Restoring the PFC deadlock detection function will also allow the PFC function to continue operating.

Example

- Re-enable the PFC function when the restore mode is set to **manual**.

```
admin@PICOS# run clear class-of-service interface xe-1/1/1 pfc-watchdog manual
```

run show pfc-watchdog stats

The **run show pfc-watchdog stats** command shows the statistics information about PFC watchdog, including the number of PFC pause storms that have been detected and restored, as well as the number of packets that have been dropped, on the PFC queues on an interface.

Command Syntax

run show pfc-watchdog stats

Parameter

Null.

Example

- View the statistics information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog stats
       QUEUE       STATUS    STORM DETECTED/RESTORED        TX OK/DROP    TX LAST OK/DROP
------------  -----------  -------------------------  ----------------  -----------------
te-1/1/25:5       stormed                        9/8      82072626556/0      32053822365/0
te-1/1/25:6       stormed                        9/8      31504345475/0      32053822365/0
te-1/1/25:7   operational                        0/0                0/0                0/0
```

In the show result,

- **STATUS**: The status of PFC watchdog. The value could be **operational** or **stormed**.
  - **operational**: Currently under detection, no deadlock found.
  - **stormed**: Currently in a deadlock state.
  - **threshold-reached**: indicates a state where the number of deadlocks has reached the upper limit within a specified time period when the deadlock restore mode is set to **auto**.
  - **manual-triggered**: indicates a state where a deadlock has occurred in the queue when the deadlock restore mode is set to **manual**.
- **STORM DETECTED**: Queue deadlock counter.
- **STORM RESTORED**: Queue Restore counter.
- **TX DROP** and **TX LAST DROP**: Number of Tx packets dropped due to PFC deadlock.
- **TX OK** and **TX LAST OK**: Number of Tx packets transmitted during deadlock (Forward action).

run show pfc-watchdog config

The **run show pfc-watchdog config** command shows the configuration information about PFC watchdog.

Command Syntax

run show pfc-watchdog config

Parameter

Null.

Example

- View the configuration information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog config
      PORT       ACTION          QUEUE    DETECTION TIME    RESTORATION TIME
----------  -----------   ------------  ----------------  ------------------
te-1/1/25          drop              6               150                 150
                                     7               150                 150
                                     6                80                  70
```

run show interface gigabit-ethernet ingress-buffer

The **run show interface gigabit-ethernet ingress-buffer** command is used to view PFC buffer information of an ingress interface, including queue ID, shared ratio, shared threshold, guaranteed threshold, reset offset and headroom threshold.

Command Syntax

run show interface gigabit-ethernet <*interface-name*> **ingress-buffer**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the name of an ingress interface with the buffer threshold configured.

Example

- View the PFC buffer information of ingress interface xe-1/1/3.

```
admin@PICOS# run show interface gigabit-ethernet xe-1/1/3 ingress-buffer
ingress_queue_id    shared_ratio    threshold    guaranteed    reset_offset    headroom
-------------------------------------------------------------------------------------
            0        none      none        none            none        none
            1        none        none      none            none        none
            2        none        none      none            none        none
            3        none        none      none            none        none
            4       none        none      none            none        none
            5       none        3000      3400            1000        none
            6       none        none      none            none        none
```

run show interface gigabit-ethernet egress-buffer

The **run show interface gigabit-ethernet egress-buffer** command is used to view PFC buffer information of an egress interface, including queue ID, shared ratio and shared threshold.

Command Syntax

run show interface gigabit-ethernet <*interface-name*> **egress-buffer**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the name of an egress interface with the buffer threshold configured.

Example

- View the PFC buffer information of egress interface xe-1/1/3.

```
admin@PICOS# run show interface gigabit-ethernet xe-1/1/3 egress-buffer
egress_queue_id    shared_ratio    threshold
-------------------------------------------
        0             none       none
        1             none       none
        2             none       none
        3             none       1000
        4             none       none
        5             none       none
        6             none       none
```

set class-of-service interface pfc-uplink-group

The **set class-of-service interface pfc-uplink-group** command creates a PFC uplink port group.

The **delete class-of-service interface pfc-uplink-group** command deletes the configuration.

> **NOTE**:
>
> Each device supports only one PFC uplink port group.

Command Syntax

set class-of-service interface *<interface-name>* **pfc-uplink-group** *<group-name>*

delete class-of-service interface *<interface-name>* **pfc-uplink-group**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies the interfaces to be added to the PFC uplink port group. The interface is a L2 physical port. **NOTE**: Routed interface and LAG interface are not allowed to be configured to the uplink port group.
pfc-uplink-group *<group-name>*	Specifies the name of the uplink port group.

Usage Guidelines

In the PFC deadlock prevention function, a PFC uplink port group is defined. For a Leaf switch, users can add the ports connected to Spine switches to the PFC uplink port group. Once the system detects that the same business flow forwarded to the ports within this port group, it indicates that the flow is a high-risk hook flow, which is prone to causing PFC deadlocks.

This command is incremental; when configured multiple times, the results are applied cumulatively.

Example

- Create a PFC uplink port group.

```
admin@PICOS# set class-of-service interface te-1/1/1 pfc-uplink-group group1
admin@PICOS# set class-of-service interface te-1/1/2 pfc-uplink-group group1
admin@PICOS# commit
```

set class-of-service pfc-uplink-group original-dscp to-code-point

The **set class-of-service pfc-uplink-group original-dscp to-code-point** command modifies the queue priority of hook flow packets that match the PFC uplink port group and the original DSCP value.

The **delete class-of-service pfc-uplink-group original-dscp to-code-point** command deletes the configuration.

> **NOTE**:
>
> - This command is supported only on the **Trident3-X5** and **Trident3-X7** platforms.
> - When configuring or deleting on the **Trident3-X5** and **Trident3-X7** platforms, the following two commands both need to be configured and submitted in the same commit.
>
> **set class-of-service pfc-uplink-group** <*group-name*> **original-dscp** <*origin-value*> **to-code-point** <*queue*>
>
> **set class-of-service pfc-uplink-group** <*group-name*> **original-dscp** <*origin-value*> **dscp** <*value*>

Command Syntax

set class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **to-code-point** <*queue*>

delete class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **to-code-point**

Parameter

Parameter	Description
pfc-uplink-group <*group-name*>	Specifies the name of the uplink port group. The value is a string.
original-dscp <*origin-value*>	Specifies the original DSCP value of the hook flow packets that matches the PFC uplink port group. The value is an integer that ranges from 0 to 63.
to-code-point <*queue*>	Specifies the adjusted queue priority of hook flow packets that match the PFC uplink port group, ensuring that the hook flow packets are forwarded from the specified queue. The value is an integer that ranges from 0 to 7.

Usage Guidelines

For hook flows that match the PFC uplink port group, the queue priority and DSCP value in the packets will be actively adjusted, changing the path of PFC pause frames to prevent PFC pause frames from forming loops.

Example

- Modify the queue priority and DSCP value of hook flow packets that match the PFC uplink port group and the original DSCP value.

```
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 to-code-point 4
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 dscp 48
```

```
admin@PICOS# commit
```

set class-of-service pfc-uplink-group original-dscp dscp

The **set class-of-service pfc-uplink-group original-dscp dscp** command modifies the DSCP value of hook flow packets that match the PFC uplink port group and the original DSCP value.

The **delete class-of-service pfc-uplink-group original-dscp dscp** command deletes the configuration.

> **NOTE**:
>
> When configuring or deleting on the **Trident3-X5** and **Trident3-X7** platforms, the following two commands both need to be configured and submitted in the same commit.
>
> **set class-of-service pfc-uplink-group** <*group-name*> **original-dscp** <*origin-value*> **to-code-point** <*queue*>
>
> **set class-of-service pfc-uplink-group** <*group-name*> **original-dscp** <*origin-value*> **dscp** <*value*>

Command Syntax

set class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **dscp** <*value*>

delete class-of-service pfc-uplink-group <*group-name*> **original-dscp** <*origin-value*> **dscp**

Parameter

Parameter	Description
pfc-uplink-group <*group-name*>	Specifies the name of the uplink port group. The value is a string.
original-dscp <*origin-value*>	Specifies the original DSCP value of the hook flow packets that matches the PFC uplink port group. The value is an integer that ranges from 0 to 63.
dscp <*value*>	Specifies the adjusted DSCP value of hook flow packets that match the PFC uplink port group, ensuring that the hook flow packets are still mapped to the designated queue on downstream devices. The value is an integer that ranges from 0 to 63.

Usage Guidelines

For hook flows that match the PFC uplink port group, the queue priority and DSCP value in the packets will be actively adjusted, changing the path of PFC pause frames to prevent PFC pause frames from forming loops.

Example

- Modify the queue priority and DSCP value of hook flow packets that match the PFC uplink port group and the original DSCP value.

```
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 to-code-point 4
admin@PICOS# set class-of-service pfc-uplink-group group1 original-dscp 32 dscp 48
admin@PICOS# commit
```

Protocol Configuration Commands

- set protocols arp interface address mac-address
- set protocols arp interface proxy
- set protocols arp inspection vlan disable
- set protocols arp inspection access-list ip mac-address
- set protocols arp inspection vlan access-list
- set protocols arp inspection trust-port
- run show arp inspection dhcp-binding
- run show arp inspection interface
- run show arp inspection vlan
- run show arp inspection access-list
- run show arp inspection statistics vlan
- set protocols arp aging-time
- set protocols lacp interface priority
- set protocols lacp priority
- set protocols sflow agent-id
- set protocols sflow collector udp-port
- set protocols sflow disable
- set protocols dhcp snooping vlan
- set protocols dhcp snooping trust-port
- set protocols dhcp snooping vlan option82-policy
- set protocols dhcp snooping option82 circuit-id
- set protocols dhcp snooping option82 remote-id
- set protocols dhcp snooping option82 trust-all
- set protocols dhcp snooping binding file
- set protocols dhcp snooping binding write-delay
- run show dhcp snooping binding
- set protocols dhcp relay interface disable
- set protocols dhcp relay interface dhcp-server-address
- set protocols dhcp relay interface relay-agent-address
- set protocols dhcp relay interface option82-policy
- set protocols dhcp relay option82 circuit-id
- set protocols dhcp relay option82 remote-id
- set protocols dhcp relay option82 trust-all
- set protocols dhcp server pool network
- set protocols dhcp server pool range low
- set protocols dhcp server pool range high
- set protocols dhcp server pool domain-name
- set protocols dhcp server pool dns-server
- set protocols dhcp server pool default-router
- set protocols dhcp server pool lease-time
- set protocols dhcp server pool vrf
- set protocols dhcp server pool tftp-server
- set protocols dhcp server pool log-server
- set protocols dhcp server pool bootfile-name
- run show dhcp server binding address
- run show dhcp server binding interface
- set protocols dhcp server interface disable
- set protocols dhcp6 relay interface disable
- set protocols dhcp6 relay interface destination
- set protocols dhcp6 relay interface remote-id
- run show dhcp6 relay-stats
- set protocols lacp interface rate
- run show lldp neighbor
- set protocols dhcp6 snooping vlan
- set protocols dhcp6 snooping trust-port
- set protocols dhcp6 snooping binding file
- set protocols dhcp6 snooping binding write-delay
- set protocols dhcp6 snooping vlan option-policy
- set protocols dhcp6 snooping option37 remote-id
- set protocols dhcp6 snooping option18 interface-id
- set protocols dhcp6 snooping interface max-clients
- run show dhcp6 snooping binding
- set protocols dhcp6 guard policy device-role

- set protocols dhcp6 guard policy trust-port
- set protocols dhcp6 guard policy interface
- set protocols dhcp6 guard policy preference-min
- set protocols dhcp6 guard policy preference-max
- set protocols dhcp6 guard policy match server source-address
- set protocols dhcp6 guard policy match reply ia-prefix
- run show dhcp6 guard policy
- run show dhcp6 guard
- run show arp
- set protocols sflow interface polling-interval
- set protocols sflow header-len
- set protocols sflow interface header-len
- set protocols sflow interfac sampling-rate egress
- set protocols sflow interface disable
- set protocols sflow interface sampling-rate ingress
- set protocols sflow polling-interval
- set protocols sflow sampling-rate egress
- set protocols sflow sampling-rate ingress
- set protocols sflow source-address

set protocols arp interface address mac-address

The **set protocols arp interface address mac-address** command configures a static ARP entry.

Command Syntax
set protocols arp interface <*interface*> **address** <*ipv4-addr*> **mac-address** <*mac-addr*>
delete protocols arp interface <*interface*> **address** <*ipv4-addr*> **mac-address** <*mac-addr*>

Parameter

Parameter	Description
interface <*interface*>	Specifies the outbound interface in a static ARP entry. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4-addr*>	Specifies the IPv4 address in a static ARP entry.
mac-address <*mac-addr*>	Specifies the MAC address in a static ARP entry.

Example

- Configure a static ARP entry that maps the IP address 10.10.60.1 to the MAC address 22:11:11:11:11:11.

```
admin@XorPlus# set protocols arp interface vlan4 address 10.10.60.1 mac-address 22:11:11:11:11:11
admin@XorPlus# commit
```

set protocols arp interface proxy

The **set protocols arp interface proxy disable** command can be used to enable or disable proxy ARP on an interface.

Command Syntax
set protocols arp interface <*interface*> **proxy disable <true | false>**
delete protocols arp interface <*interface*> **proxy**

Parameter

Parameter	Description
interface <*interface*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <true | false>	Enables or disables proxy ARP. The value could be **true** or **false**. • **true**: Disables proxy ARP. • **flase**: Enables proxy ARP.

Example

- Enable proxy ARP on vlan4:

```
admin@XorPlus# set protocols arp interface vlan4 proxy disable false
admin@XorPlus# commit
```

set protocols arp inspection vlan disable

The **set protocols arp inspection vlan disable** command enables or disables ARP inspection in a VLAN.

Command Syntax

set protocols arp inspection vlan <*vlan-id*> **disable** <**true | false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true	false**>	Enables or disables the ARP inspection. The value could be **true** or **false**. • **true**: disables the ARP inspection function. • **false**: enables the ARP inspection function. By default, ARP inspection function is disabled.

Usage Guidelines

When ARP inspection is enabled in a VLAN, the device checks ARP packets received on interfaces belong to the VLAN based on the static access lists (if configured) and the DHCP binding table except when the interface is a trust port (configured by using command **set protocols arp inspection trust-port** <*port-name*>).

NOTE:

Regardless of the fact that whether its static access lists or dynamic ARP inspection, you have to explicitly enable the ARP inspection function in the VLAN by using this command.

Example

- Enable ARP inspection in VLAN 100.

```
admin@XorPlus# admin@Xorplus# set protocols arp inspection vlan 100 disable false
admin@XorPlus# commit
```

set protocols arp inspection access-list ip mac-address

The **set protocols arp inspection access-list ip mac-address** command configures an ARP access list for ARP inspection.

NOTE:

When configuring the static access list for ARP Inspection, the same IP-MAC cannot exist in multiple access lists.

Command Syntax

set protocols arp inspection access-list <*acl-name*> **ip** <*ipv4-addr*> **mac-address** <*mac-addr*>

Parameters

Parameter	Description
access-list <*acl-name*>	Specifies access list name. The value is a string.
ip <*ipv4-addr*>	Specifies the IP address in a static ARP binding entry. The value is in dotted decimal notation.
mac-address <*mac-addr*>	Specifies the MAC address in a static ARP binding entry. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. Note that, the MAC address cannot be configured to a multicast MAC or the system MAC.

Example

- Configure a static access list of ARP inspection that maps the IP address 10.0.0.1 to the MAC address 00:B0:BC:00:00:00.

```
admin@Xorplus# set protocols arp inspection access-list test1 ip 10.0.0.1 mac-address 00:B0:BC:00:00:00
admin@Xorplus# commit
```

set protocols arp inspection vlan access-list

The **set protocols arp inspection vlan access-list** command applies an ARP inspection access list to a VLAN.

Command Syntax

set protocols arp inspection vlan <*vlan-id*> **access-list** <*acl-name*>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
access-list <*acl-name*>	Specifies an access list name. The value is a string.

Usage Guidelines

A VLAN can be configured with multiple access-lists, and the system will check through the access-lists of the VLAN to match an ARP entry upon receiving an ARP packet. If no ARP entry is matched, the ARP packet will be dropped.

NOTE:

Configure the access-list first and then apply to a VLAN, otherwise it will prompt access-list does not exist when committing this command.

Example

- Apply the ARP inspection access list test1 to VLAN 100.

```
admin@Xorplus# set protocols arp inspection vlan 100 access-list test1
admin@Xorplus# commit
```

set protocols arp inspection trust-port

The **set protocols arp inspection trust-port** command configures an interface as a trust port on which ARP inspection will not be implemented.

Command Syntax

set protocols arp inspection trust-port <*port-name*>

Parameters

Parameter	Description
trust-port <*port-name*>	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces for ARP inspection.

Usage Guidelines

ARP inspection divides interfaces into trusted and untrusted ports. On trusted ports, the system does not perform ARP inspection on incoming ARP messages, allowing the ARP messages to pass. However, ARP inspection is required for ARP messages received on the untrusted port interface.

You can use the command **run show arp inspection interface** to show the trust state of all the interfaces for ARP inspection.

Example

- Configure the interface ge-1/1/1 as an ARP inspection trust port.

```
admin@Xorplus# set protocols arp inspection trust-port ge-1/1/1
admin@Xorplus# commit
```

run show arp inspection dhcp-binding

The **run show arp inspection dhcp-binding** command displays the ARP inspection table. This table includes the ARP entries generated from the DHCP snooping or DHCP relay table.

Command Syntax

run show arp inspection dhcp-binding

Parameter

None.

Example

- Display the ARP inspection table.

```
admin@Xorplus# run show arp inspection dhcp-binding
Vlan  IP Address      Mac Address
----  --------------  -----------------
 2    100.1.1.1     14:18:77:18:2c:b9
```

run show arp inspection interface

The **run show arp inspection interface** command displays the trust state of all the interfaces for ARP inspection.

Command Syntax

run show arp inspection interface

Parameter

None.

Example

- Display the trust state of all the interfaces for ARP inspection.

```
admin@Xorplus# run show arp inspection interface
Interface   Trust State
----------  -----------
ge-1/1/1    Untrusted
ge-1/1/2    Trusted
...
ge-1/1/47   Untrusted
ge-1/1/48   Untrusted
te-1/1/1    Untrusted
te-1/1/2    Untrusted
```

Table 1 Description of the **run show arp inspection interface** command output

Item	Description
Interface	Indicates the interface name.
Trust State	Indicates the trust state of all the interfaces for ARP inspection. The value could be **Untrusted** or **Trusted**. The value is **Trusted** if the interface has been configured as trust port by using the command **set protocols arp inspection trust-port** <*port-name*>. Else, it prints **Untrusted**.

run show arp inspection vlan

The **run show arp inspection vlan** command displays ARP inspection configured information of a VLAN, such as, the configured static access lists of ARP inspection in the VLAN.

Command Syntax

run show arp inspection vlan <*vlan-id*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094. **Note**: you shold firstly use command **set protocols arp inspection vlan** to bind ARP inspection and VLAN ID, or *vlan-id* cannot be set.

Example

- Display the configured static access lists of ARP inspection in VLAN 100.

```
admin@Xorplus# run show arp inspection vlan 100
Vlan  Configuration  Static ACL
----  -------------  ----------
100   Enabled        abc
                     bbb
```

Table 1 Description of the **run show arp inspection vlan** command output

Item	Description
Vlan	Indicates the VLAN ID.
Configuration	Indicates whether ARP inspection is enabled in the VLAN. The value could be **Enabled** or **Disabled**.
Static ACL	Indicates static access lists of ARP inspection in the VLAN if configured.

run show arp inspection access-list

The **run show arp inspection access-list** command displays the binding entries and applied VLANs of a static access list of ARP inspection.

Command Syntax

run show arp inspection access-list [*<acl-name>*]

Parameter

Parameter	Description
<acl-name>	Optional. Specifies access list name. The value is a string. If you do not specify an access list name, then display all configured access list; if an access list name is specified, then display configuration information of the specific access list.

Example

- Display the binding entries of the static access list test1 of ARP inspection.

```
admin@Xorplus# run show arp inspection access-list test1
Static ACL  IP Address       Mac Address
----------  ---------------  -----------------
Test1       1.1.22.1         00:00:00:00:00:11
            1.1.30.1         00:00:00:00:22:11
Static ACL  Applied Vlans
----------    ------------------
Test1       100  200  300  400
            500  600  700  800
            900  4000
```

- Display the binding entries of all the static access lists of ARP inspection.

```
admin@Xorplus# run show arp inspection access-list
Static ACL  IP Address       Mac Address
----------  ---------------  -----------------
abc         1.1.22.1         00:00:00:00:00:11
            1.1.30.1         00:00:00:00:22:11
bbb         1.1.11.1         00:00:00:22:22:11
```

Table 1 Description of the **run show arp inspection access-list** command output

Item	Description
Static ACL	Indicates the access list name.
IP Address	Indicates the IP address in a static ARP binding entry.
Mac Address	Indicates the MAC address in a static ARP binding entry.
Applied Vlans	Indicates the VLANs to which the static access list is applied to.

run show arp inspection statistics vlan

The **run show arp inspection statistics vlan** command displays the statistics of ARP inspection, such as, discarded and permitted ARP packets.

Command Syntax

run show arp inspection statistics vlan <*vlan-id*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094. **Note**: you shold firstly use command **set protocols arp inspection vlan** to bind ARP inspection and VLAN ID, or *vlan-id* cannot be set.

Example

- Displays the statistics on discarded and permitted ARP packets by ARP inspection in VLAN 100.

```
admin@Xorplus# run show arp inspection statistics vlan 100
Vlan  Total Count  IP Validation Failures  MAC Validation Failures
----  -----------  ----------------------  -----------------------
100   10453        0                       0
Vlan  DHCP Drops  DHCP Permits  ACL Drops  ACL Permits
----  ----------  ------------  ---------  -----------
100   0           0             0          10453
```

Table 1 Description of the **run show arp inspection statistics vlan** command output

Item	Description
Vlan	Indicates the VLAN ID.
Total Count	Total number of the received ARP packets.
IP Validation Failures	Number of invalid IP addresses carried in incoming ARP messages, including multicast, broadcast and all 0 IP addresses.
MAC Validation Failures	Number of invalid MAC addresses carried in incoming ARP messages, including multicast MACs, broadcast MAC addresses, system MAC address, all 0 addresses and other invalid MAC addresses. Other invalid MAC addresses are ARP messages in which the source MAC address in the ARP message and the source MAC address in the Ethernet header are consistent.
DHCP Drops	Number of discarded ARP packets that matched no DHCP snooping binding entry.
DHCP Permits	Number of permitted ARP packets that matched the DHCP snooping binding entries.
ACL Drops	Number of discarded ARP packets that matched no entry of ARP inspection static access list.
ACL Permits	Number of permitted ARP packets that matched the entries of ARP inspection static access list.

set protocols arp aging-time

The Address Resolution Protocol (ARP) maps an IP address to a MAC address to enable communications within an IP network broadcast domain. If a given host (A) does not have the MAC address of another host (B) with which it wants to communicate, the sending host will generate a broadcast message to all hosts within the broadcast domain in order to obtain the MAC address of host B. While all hosts will receive the ARP request, only host B will respond with its MAC address. Host A will then cache the MAC address for future use. ARP aging is used to set the amount of time the address will remain in that cache. The default ARP aging time is 1200 seconds. This document describes how to change the ARP aging time.

Command Syntax
set protocols arp aging-time <*seconds*>
delete protocols arp aging-time

Parameters

Parameter	Description
aging-time <*seconds*>	Aging time in seconds,[300..14400]

Example
• This example is to set arp aging time to 400:

```
admin@XorPlus# set protocols arp aging-time 400
admin@XorPlus# commit
```

set protocols lacp interface priority

Users can set link aggregation option of gigabit-ethernet interface.

Command Syntax
set protocols lacp interface <*interface*> **priority** <*value*>
delete protocols lacp interface <*interface*> **priority**

Parameters

Parameter	Description
interface <*interface*>	Link aggregation option of gigabit-ethernet interface (e.g. ge-1/1/1)
priority <*value*>	Priority value, [0..65535]

Example
• This example is to set lacp priority of ge-1/1/1 to 3000 :

```
admin@XorPlus# set protocols lacp interface ge-1/1/1 priority 3000
admin@XorPlus# commit
```

set protocols lacp priority

Users can configure the lacp priority of system.

Command Syntax
set protocols lacp priority <*value*>
delete protocols lacp priority

Parameters

Parameter	Description
priority <*value*>	Priority value, [0..65535]

Example
• This example is to set priorit of system to 1000:

```
admin@XorPlus# set protocols lacp priority 1000
admin@XorPlus# commit
```

set protocols sflow agent-id

Users can set agent-id for sflow interface.

Command Syntax
set protocols sflow agent-id <*IPv4*>

Parameter

Parameter	Description
agent-id <*IPv4*>	A unique 32-bit identifier of the agent.

Example
• This example is to set agent-id to 10.10.50.248:

```
admin@XorPlus# set protocols sflow agent-id 10.10.50.248
admin@XorPlus# commit
```

set protocols sflow collector udp-port

Users can set sFlow collector IPv4 address.

Command Syntax
set protocols sflow collector *<IPv4>* **udp-port** *<port>*
delete protocols sflow collector *<IPv4>*

Parameter

Parameter	Description
collector *<IPv4>*	Configure the collector.
udp-port *<port>*	The UDP port of the collector, 6343 by default.

Usage Guidelines

To change the upd-port for a collector, you have to delete the collector configuration first and then set it back with the new upd-port.

For example,

Assume the original configuration as follows:

set protocols sflow collector 10.10.51.42 udp-port 3355

The following commands change the udp-port to 3366.

```
admin@Xorplus# delete protocols sflow collector 10.10.51.42
admin@Xorplus# commit
admin@Xorplus# set protocols sflow collector 10.10.51.42 udp-port 3366
admin@Xorplus# commit
```

Example
• This example is to configure the collector as 10.10.50.221,udp-port is 6343:

```
admin@XorPlus# set protocols sflow collector 10.10.50.221 udp-port 6343
admin@XorPlus# commit
```

set protocols sflow disable

By default, sFlow is disabled. Users can enable sFlow and configure its' parameters.

Command Syntax
set protocols sflow disable [**true** | **false**]
delete protocols sflow disable

Parameter

Parameter	Description
[**true** | **false**]	Disable sflow on all interfaces by default. • **true**: Disable sflow • **false**: enable sflow

Example
• This example is to enable sflow on all interface:

```
admin@XorPlus# set protocols sflow disable false
admin@XorPlus# commit
```

set protocols dhcp snooping vlan

The **set protocols dhcp snooping vlan disable** command enables DHCP snooping in a specified VLAN.

Command Syntax

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true** | **false**>	Enables or disables DHCP snooping, the value could be **true** or **false**: • **true**: Disables DHCP snooping. • **false**: Enables DHCP snooping. By default, DHCP snooping is disabled.

Usage Guidelines

DHCP snooping should be enabled in the VLAN, it takes effect only on the DHCP messages received from the VLAN enabled with DHCP snooping function. Packets received from the VLANs with DHCP snooping disabled will not be processed by the DHCP snooping module, and they will be processed and forwarded by the device as ordinary packets.

NOTE:

- The DHCP snooping function is only practicable to the clients directly connected to the local L2 domain, rather than connected through a router.
- When DHCP snooping is disabled, the DHCP binding entry for the VLAN will be removed correspondingly.

Example

- Enable DHCP snooping in VLAN 12.

```
admin@Xorplus# set protocols dhcp snooping vlan 12 disable false
admin@Xorplus# commit
```

set protocols dhcp snooping trust-port

The **set protocols dhcp snooping trust-port** command configures an interface as a trust interface for DHCP snooping.

Command Syntax

set protocols dhcp snooping trust-port <*interface-name*>

Parameters

Parameter	Description
trust-port <*interface-name*>	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces.

Usage Guidelines

In order to make the DHCP client obtain an IP address from a legitimate DHCP server, the device interface directly or indirectly connected to the DHCP server trusted by the administrator must be set to the trust interface, so as to prevent a spoofing DHCP server from assigning an IP address to the DHCP client.

The trusted interface forwards DHCP packets received from the DHCP server normally, whereas the untrusted interface discards DHCP ACK and DHCP OFFER packets received from the DHCP server.

Example

- Configure ge-1/1/1 as trust port for DHCP snooping.

```
admin@Xorplus# set protocols dhcp snooping trust-port ge-/1/1/1
admin@Xorplus# commit
```

set protocols dhcp snooping vlan option82-policy

The **set protocols dhcp snooping vlan option82-policy** command configures how to handle the Option 82 field when receiving a DHCP Discover/Request/Release/Decline/Inform message with Option 82 on VLANs where DHCP snooping is enabled.

Command Syntax

set protocols dhcp snooping vlan <*vlan-id*> **option82-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
option82-policy <**drop	keep	insert	replace**>	Specifies the policy for Option 82. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 82. If the received DHCP packets have no Option 82 values, the packets will be forwarded. • **keep**: Option 82 in the packet remains unchanged and forwarded. • **insert**: the existing Option 82 sub-options remain unchanged, and the non-existing Option 82 sub-options will be inserted with the value the administrator configured, then forward the packet to the DHCP server. • **replace**: The non-existing Option 82 sub-options, will be inserted with the value the administrator configured. The existing Option 82 sub-options will be replaced with the value administrator configured, and then forward the packet. The default value is **keep**.

Usage Guidelines

Option 82 policy is used when receiving a DHCP Discover/Request/Release/Decline/Inform message from the DHCP client. When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of circuit ID and remote ID sub-options:

set protocols dhcp snooping option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp snooping option82 remote-id <**system-mac | hostname**>

We can use the following table to summarize the Option 82 policy.

Received Packet / Option82 Policy	No Option82	Only Circle ID	Only Remote ID	Circle ID + Remote ID
drop	The packet is forwarded without changing option 82.	The packet is dropped.	The packet is dropped.	The packet is dropped.
keep	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.
insert	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: unchanged. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: unchanged.	The packet is forwarded. Circle ID: unchanged. Remote ID: unchanged.
replace	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: replaced with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: replaced with the value configured.

For details about how Option 82 is processed by the DHCP snooping and DHCP relay module, see Introduction to DHCP.

Example

- Configure the Option 82 policy.

```
admin@Xorplus# set protocols dhcp snooping vlan 12 option82-policy insert
admin@Xorplus# commit
```

set protocols dhcp snooping option82 circuit-id

The **set protocols dhcp snooping option82 circuit-id** command configures the format of sub-option circuit ID inserted into the Option 82 field for DHCP snooping.

NOTE: The sub-option circuit ID is applied to VLANs where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp snooping option82 circuit-id <**port-index** | **port-name** | **port-description**>

Parameters

Parameter	Description
circuit-id <**port-index	port-name	port-description**>	Specifies the type of circuit ID in the Option 82 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option circuit ID is not configured which means circuit ID is not enabled.

Usage Guidelines

If configured, the circuit ID is filled with the port identifier and VLAN.

- When “port-index” is selected, the format of the circuit ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the circuit ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the circuit ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernet *<lag_name>* **description** *<description>*

set interface gigabit-ethernet *<physical-port>* **description** *<description>*

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of the sub-option circuit ID for the Option 82 field.

```
admin@Xorplus# set protocols dhcp snooping option82 circuit-id port-index
admin@Xorplus# commit
```

set protocols dhcp snooping option82 remote-id

The **set protocols dhcp snooping option82 remote-id** command configures the format of sub-option remote ID inserted into the DHCP Option 82 field for DHCP snooping.

NOTE: The sub-option remote ID is applied to VLANs where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp snooping option82 remote-id <**system-mac** | **hostname**>

Parameters

Parameter	Description
remote-id <system-mac | hostname>	Specifies the type of remote ID in the Option 82 field. The value could be **system-mac** or **hostname**. By default, the sub-option remote ID is not configured which means remote ID is not enabled.

Usage Guidelines

If configured, the remote ID is unique per switch.

- When “system-mac” is selected, the format of the remote ID is “system MAC”.
- When “hostname” is selected, the format of the remote ID is “hostname”. The value of “hostname” can be set by the following command:

set system hostname <*hostname*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the type of sub-option remote ID inserted into the DHCP Option 82 field.

```
admin@Xorplus# set protocols dhcp snooping option82 remote-id system-mac
admin@Xorplus# commit
```

set protocols dhcp snooping option82 trust-all

The **set protocols dhcp snooping option82 trust-all** command is used to enable or disable Option 82 trust-all function for DHCP snooping.

Command Syntax

set protocols dhcp snooping option82 trust-all <**true | false**>

Parameters

Parameter	Description
<**true** | **false**>	Enables or disables Option 82 trust-all function, the value could be **true** or **false**: • **true**: Enables Option 82 trust-all function. • **false**: Disables Option 82 trust-all function. By default, Option 82 trust-all function is disabled.

Usage Guidelines

DHCP Discover/Request/Release/Decline/Inform packets received on the switch without giaddr but containing Option 82 are dropped by default. To allow these packets on the switch, PICOS supports Option 82 trust all function:

- If trust all is enabled, such packets will be processed according to the configuration of the Option 82 policy.
- If trust all is disabled, then drop the packets.

This command is useful if there is a switch in between the client and the DHCP snooping device that may insert Option 82. Use this command to ensure that these packets do not get dropped.

Example

- Enable Option 82 trust-all function.

```
admin@Xorplus# set protocols dhcp snooping option82 trust-all true
admin@Xorplus# commit
```

set protocols dhcp snooping binding file

The **set protocols dhcp snooping binding file** command configures a DHCP snooping binding file for synchronizing DHCP snooping entries from memory.

Command Syntax

set protocols dhcp snooping binding file <*file-path*>

Parameters

Parameter	Description
file <*file-path*>	Specifies a file path to save the DHCP snooping binding table.

Usage Guidelines

If a DHCP snooping binding file is specified, the DHCP snooping entries will be synchronized from the memory to the binding file. This prevents DHCP snooping entries data loss in case of power failure. By setting a DHCP snooping binding file, the system can directly load the existing snooping entries from the binding file after if recovers.

Example

- Configure the DHCP snooping binding file.

```
admin@Xorplus# set protocols dhcp snooping binding file /tmp/run/dhcp_bind
admin@XorPlus# commit
```

set protocols dhcp snooping binding write-delay

The **set protocols dhcp snooping binding write-delay** command configures a delay timer for writing the DHCP snooping entries from memory to the binding file.

Command Syntax

set protocols dhcp snooping binding write-delay <*write-delay-timer*>

Parameters

Parameter	Description
write-delay <*write-delay-timer*>	Specifies a delay timer for writing the DHCP snooping entries from the memory to the binding file. The value is an integer in seconds that ranges from 15 to 86400. The default value is 300s.

Usage Guidelines

In order to reduce the system burden caused by frequent file writes, you can configure a delay timer for writing the DHCP snooping entries from memory to the binding file.

NOTE:

In the case when the DHCP snooping entry is changed by the administrator configuration modifications from the CLI, such as modifying the VLAN, the binding file will be immediately refreshed rather than wait for write-delay timer.

Example

- Configure a delay timer for writing the DHCP snooping entries from memory to the binding file.

```
admin@Xorplus# set protocols dhcp snooping binding write-delay 24
admin@XorPlus# commit
```

run show dhcp snooping binding

The **run show dhcp snooping binding** command displays the DHCP snooping binding table, which includes the user MAC address, IP address, VLAN ID, access interface and the lease time.

Command Syntax

run show dhcp snooping binding

Parameter

None.

Example

- Show the DHCP snooping binding table.

```
admin@Xorplus# run show dhcp snooping binding
Total count:     2
MAC Address         IP Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------
e4:f0:04:89:b6:46   0.0.0.0         ae65            1         0/0
14:18:77:18:2c:b9   100.1.1.1       ae25            125       599/600
```

Table 1. Description of the run show dhcp snooping binding command output

Item	Description
Mac Address	User MAC address.
IP Address	User IP address.
Port	User access interface.
VLAN ID	User VLAN ID.
Lease(sec)	Lease time for the IP address, in seconds. The format displayed is **Remaining Lease Time/Total Lease Time**.

set protocols dhcp relay interface disable

The **set protocols dhcp relay interface disable** command enables or disables DHCP relay on a specified L3 interface.

Command Syntax

set protocols dhcp relay interface <*l3-interface-name*> **disable <true | false>**

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <**true** | **false**>	Enables or disables DHCP relay on an L3 interface, the value could be **true** or **false**: • **true**: Disables DHCP relay. • **false**: Enables DHCP relay. By default, DHCP relay is disabled.

Usage Guidelines

Generally, DHCP relay should be enabled on the L3 interface that connects to the host's network.

Example

- Enable DHCP relay on the L3 VLAN interface vlan100.

```
admin@Switch# set protocols dhcp relay interface vlan100 disable false
admin@Switch# commit
```

set protocols dhcp relay interface dhcp-server-address

The **set protocols dhcp relay interface dhcp-server-address** command configures a DHCP server address on the L3 interface enabled with DHCP relay.

Command Syntax

set protocols dhcp relay interface *<l3-interface-name>* **dhcp-server-address** *<server-ipv4-address>*

Parameters

Parameter	Description
interface *<l3-interface-name>*	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dhcp-server-address *<server-ipv4-address>*	Specifies the IPv4 address of a DHCP server. The value is in dotted decimal notation.

Usage Guidelines

You can repeat this command to configure multiple DHCP servers.

NOTE: The DHCP server IP address should not be in the same subnet with the L3 interface enabled with the DHCP relay.

Example

- Configure DHCP relay and DHCP server address on L3 VLAN interface vlan100.

```
admin@Xorplus# set protocols dhcp relay interface vlan100 dhcp-server-address 10.10.1.1
admin@Xorplus# commit
```

set protocols dhcp relay interface relay-agent-address

The **set protocols dhcp relay interface relay-agent-address** command configures the IP address of the DHCP relay agent.

Command Syntax

set protocols dhcp relay interface *<l3-interface-name>* **relay-agent-address** *<agent-ipv4-address>*

Parameters

Parameter	Description
interface *<l3-interface-name>*	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
relay-agent-address *<agent-ipv4-address>*	Specifies the IP address of the DHCP relay agent. The value is in dotted decimal notation.

Usage Guidelines

DHCP relay agent address is a required configuration in VRRP topology, when the VRRP Master/Backup devices are used as the DHCP relay agents, you must configure the DHCP relay agent address to the virtual IP address of the VRRP group.

The interface name here should be configured with the L3 interface which is enabled with DHCP relay and VRRP group.

However, in a non-VRRP topology, there's no need to configure the DHCP relay agent address. By default, the system sets the IP address of the L3 interface that is enabled with the DHCP relay as the DHCP relay agent address.

The system supports multiple DHCP relay agent addresses on a switch, one DHCP relay agent address for each VRRP group.

Example

- Con*figure a DHCP relay agent address* on L3 VLAN interface vlan100.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5
admin@Xorplus# set protocols dhcp relay interface vlan100 relay-agent-address 192.168.1.5
admin@Xorplus# commit
```

set protocols dhcp relay interface option82-policy

The **set protocols dhcp relay interface option82-policy** command configures how to handle the Option 82 field when receiving a DHCP Discover, DHCP Request, DHCP Release, DHCP Decline or DHCP Inform message with Option 82 on the L3 interfaces where DHCP relay is enabled.

Command Syntax

set protocols dhcp relay interface *<l3-interface-name>* **option82-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
interface *<l3-interface-name>*	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
option82-policy <drop | keep | insert | replace>	Specifies the policy for Option 82. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 82. If the received DHCP packets have no Option 82 values, the packets will be forwarded. • **keep**: Option 82 in the packet remains unchanged and forwarded. • **insert**: the existing Option 82 sub-options remain unchanged, and the non-existing Option 82 sub-options will be inserted with the value the administrator configured, then forward the packet to the DHCP server. • **replace**: The non-existing Option 82 sub-options, will be inserted with the value the administrator configured. The existing Option 82 sub-options will be replaced with the value administrator configured, and then forward the packet. The default value is **keep**.

Usage Guidelines

Option 82 policy is used when receiving a DHCP Discover/Request/Release/Decline/Inform message from the DHCP client. When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of sub-option circuit ID and remote ID:

set protocols dhcp relay option82 circuit-id <port-index | port-name | port-description>

set protocols dhcp relay option82 remote-id <system-mac | hostname>

We can use the following table to summarize the Option 82 policy.

Received Packet / Option82 Policy	No Option82	Only Circle ID	Only Remote ID	Circle ID + Remote ID
drop	The packet is forwarded without changing option 82.	The packet is dropped.	The packet is dropped.	The packet is dropped.
keep	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.
insert	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: unchanged. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: unchanged.	The packet is forwarded. Circle ID: unchanged. Remote ID: unchanged.
replace	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: replaced with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: replaced with the value configured.

For details about how Option 82 is processed by the DHCP snooping and DHCP relay module, see Introduction to DHCP.

Example

- Configure the Option 82 policy.

```
admin@Xorplus# set protocols dhcp relay interface vlan12 option82-policy insert
admin@Xorplus# commit
```

set protocols dhcp relay option82 circuit-id

The **set protocols dhcp relay option82 circuit-id** command configures the format of sub-option circuit ID inserted into the DHCP Option 82 field for DHCP relay.

NOTE: The sub-option circuit ID is applied to VLAN interfaces where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp relay option82 circuit-id <**port-index** | **port-name** | **port-description**>

Parameters

Parameter	Description
circuit-id <port-index | port-name | port-description>	Specifies the format of circuit ID in the Option 82 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option circuit ID is not configured, which means circuit ID is not enabled.

Usage Guidelines

If configured, the circuit ID is filled with port identifier and VLAN:

- When “port-index” is selected, the format of the circuit ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the circuit ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the circuit ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernett <*lag_name*> **description** <*description*>

set interface gigabit-ethernet <*physical-port-name*> **description** <*description*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of sub-option circuit ID in the Option 82 field to port-index.

```
admin@Xorplus# set protocols dhcp relay option82 circuit-id port-index
admin@Xorplus# commit
```

set protocols dhcp relay option82 remote-id

The **set protocols dhcp relay option82 remote-id** command configures the format of sub-option remote ID inserted into the DHCP Option 82 field for DHCP relay.

NOTE: The sub-option remote ID is applied to VLAN interfaces where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp relay option82 remote-id <**system-mac** | **hostname**>

Parameters

Parameter	Description
remote-id <system-mac | hostname>	Specifies the format of remote ID in the Option 82 field. The value could be **system-mac** or **hostname**. By default, the sub-option remote ID is not configured, which means remote ID is not enabled.

Usage Guidelines

If configured, the remote ID is unique per switch.

- When “system-mac” is selected, the format of the remote ID is “system MAC”.
- When “hostname” is selected, the format of the remote ID is “hostname”. The value of “hostname” can be set by the system hostname command:

set system hostname <*hostname*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of sub-option remote ID inserted into the DHCP Option 82 field.

```
admin@Xorplus# set protocols dhcp relay option82 remote-id system-mac
admin@Xorplus# commit
```

set protocols dhcp relay option82 trust-all

The **set protocols dhcp relay option82 trust-all** command is used to enable or disable Option 82 trust-all function for DHCP relay.

Command Syntax

set protocols dhcp relay option82 trust-all <**true | false**>

Parameters

Parameter	Description
<**true** | **false**>	Enables or disables Option 82 trust-all function, the value could be **true** or **false**: • **true**: Enables Option 82 trust-all function. • **false**: Disables Option 82 trust-all function. By default, Option 82 trust-all function is disabled.

Usage Guidelines

DHCP Discover/Request/Release/Decline/Inform packets received on the switch without giaddr but containing Option 82 are dropped by default. To allow these packets on the switch, PICOS supports Option 82 trust all function:

- If trust all is enabled, such packets will be processed according to the configuration of the Option 82 policy.
- If trust all is disabled, then drop the packets.

This command is useful if there is a switch in between the client and the relay agent that may insert Option 82. Use this command to ensure that these packets do not get dropped.

Example

- Enable Option 82 trust-all function.

```
admin@Xorplus# set protocols dhcp relay option82 trust-all true
admin@Xorplus# commit
```

set protocols dhcp server pool network

The **set protocols dhcp server pool network** command creates an IPv4 address pool and the network that can be assigned to the DHCP clients.

Command Syntax

set protocols dhcp server pool <*pool-name*> **network** <*IPv4Net*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
network <*IPv4Net*>	Specify an IPv4 network segment from which DHCP server can dynamically assign IP addresses to the DHCP clients. The value is in the form of *IPv4_address/ prefix_length*, where *prefix_length* can range from 1 to 32. For example, 10.10.10.0/24.

Usage Guidelines

The DHCP server can assign IP addresses to the DHCP clients from the configured address pool.

NOTE:

- Each address pool can be configured with only one network segment. If the system needs multiple segments, multiple address pools need to be configured, but there can be no address overlap between pools.
- The network segment of the address pool should be the same network segment as the IP of the VLAN interface connected to the client.

Example

- Create an IPv4 address pool pool1, and the network is 10.1.10.0/24.

```
admin@Xorplus# set protocols dhcp server pool pool1 network 10.1.10.0/24
admin@Xorplus# commit
```

set protocols dhcp server pool range low

The **set protocols dhcp server pool range low** command configures the lower boundary of a range of addresses in the address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **low** <*ipv4-address*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
range <*range-name*>	Specifies a range name of addresses. The value is a string of case-sensitive characters, spaces are not supported.
low <*ipv4-address*>	Specifies the lower boundary of a range of addresses. The value is in dotted decimal notation.

Usage Guidelines

This command should be configured together with the command **set protocols dhcp server pool** <*pool-name*> **range** <*range-name*> **high** <*ipv4-address*>, separately configuring the lower and upper boundaries of an address range of an address pool. The address range is required to be a subnet of the address pool.

NOTE:

- The address range is optional. If not configured, it means that all the IP addresses in the address pool are available for address assignment. However, if configured, only addresses in the range are used for address assignment.
- When multiple address ranges are configured under an address pool, there should be no address overlap between different ranges.

Example

- Configure a range of addresses.

```
admin@Xorplus# set protocols dhcp server pool pool1 range range1 low 10.1.10.2
admin@Xorplus# set protocols dhcp server pool pool1 range range1 high 10.1.10.225
admin@Xorplus# commit
```

set protocols dhcp server pool range high

The **set protocols dhcp server pool range high** command configures the upper boundary of a range of addresses in the address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **high** <*ipv4-address*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
range <*range-name*>	Specifies a range name of addresses. The value is a string of case-sensitive characters, spaces are not supported.
high <*ipv4-address*>	Specifies the upper boundary of a range of addresses. The value is in dotted decimal notation.

Usage Guidelines

This command should be configured together with the command **set protocols dhcp server pool** <*pool-name*> **range** <*range-name*> **low** <*ipv4-address*>, separately configuring the lower and upper boundaries of an address range of an address pool. The address range is required to be a subnet of the address pool.

NOTE:

- The address range is optional. If not configured, it means that all the IP addresses in the address pool are available for address assignment. However, if configured, only addresses in the range are used for address assignment.
- When multiple address ranges are configure under an address pool, there should be no address overlap between different ranges.

Example

- Configure a range of addresses.

```
admin@Xorplus# set protocols dhcp server pool pool1 range range1 low 10.1.10.2
admin@Xorplus# set protocols dhcp server pool pool1 range range1 high 10.1.10.225
admin@Xorplus# commit
```

set protocols dhcp server pool domain-name

The **set protocols dhcp server pool domain-name** command configures a DNS domain name assigned to a DHCP client.

Command Syntax

set protocols dhcp server pool <*pool-name*> **domain-name** <*domain-name*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
domain-name <*domain-name*>	Specifies a domain name to be assigned to a DHCP client. The value is a string of 1 to 128 characters without spaces.

Usage Guidelines

On the DHCP server, use the command **set protocols dhcp server pool** <*pool-name*> **domain-name** <*domain-name*> to specify the domain name suffix to assign to the DHCP client for each address pool. The DHCP server sends the domain name to the client when allocating IP address to the client.

Example

- Configure a DNS domain name.

```
admin@Xorplus# set protocols dhcp server pool pool1 domain-name company.com
admin@Xorplus# commit
```

set protocols dhcp server pool dns-server

The **set protocols dhcp server pool dns-server** command configures a DNS server address for an address pool.

Command Syntax

run show vrf

set protocols dhcp server pool <*pool-name*> **dns-server** <*dns-server-ip*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
dns-server <*dns-server-ip*>	Specifies the DNS server address. The value is in dotted decimal notation.

Usage Guidelines

DNS servers are used for domain name resolution. To enable DHCP clients to communicate with devices on other networks through host names, configure the DNS server.

To enable DNS services for the DHCP client, specify the DNS server address for the address pool on the DHCP server. When allocating IP address to the client, the DHCP server sends the DNS server address to the client.

Repeatedly configure this command to configure multiple DNS servers. Each address pool can be configured with a maximum of eight DNS server addresses.

Example

- Configure a DNS server address for an address pool.

```
admin@Xorplus# set protocols dhcp server pool pool1 dns-server 10.3.10.1
admin@Xorplus# commit
```

set protocols dhcp server pool default-router

The **set protocols dhcp server pool default-router** command configures a default gateway address for the DHCP clients.

Command Syntax

set protocols dhcp server pool *<pool-name>* **default-router** *<router-ip address>*

Parameter

Parameter	Description
pool *<pool-name>*	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
default-router *<router-ip address>*	Specifies an egress gateway address. The value is in dotted decimal notation.

Usage Guidelines

In order to allow the DHCP client to access the network normally, the default gateway can be configured for the DHCP clients to send and receive user data.

Example

- Configure a default gateway address for the DHCP clients.

```
admin@Xorplus# set protocols dhcp server pool pool1 default-router 10.10.10.1
admin@Xorplus# commit
```

set protocols dhcp server pool lease-time

The **set protocols dhcp server pool lease-time** command configures the lease time for IP addresses in an address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **lease-time** <*lease-time*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
lease-time <*lease-time*>	Specifies the lease time for IP addresses. The value is an integer that ranges from 2 to 4294967295, in minute. The default value is 60 minutes.

Example

- Configure the lease for IP addresses in an address pool to two days.

```
admin@Xorplus# set protocols dhcp server pool pool2 lease-time 2880
admin@Xorplus# commit
```

set protocols dhcp server pool vrf

The **set protocols dhcp server pool vrf** command assigns a DHCP address pool to a VRF.

Command Syntax

set protocols dhcp server pool <*pool-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string of case-sensitive characters, spaces are not supported.

Usage Guidelines

In most cases, one address pool allocates IP addresses to clients in only one network segment to prevent IP address conflicts. However, in VRF scenario, different VRFs can use IP addresses on the same network segment. This command can be used to assign different DHCP address pools to different VRFs.

To enable the IP address allocation on the same network segment in two different VRFs, first you have to configure two different pools with the same network segment, and then assign the DHCP address pools to different VRFs separately.

NOTE:

- If a pool is not associated with any specific VRF, by default, it is assigned to the default VRF.
- Each pool can only be assigned to one VRF, but each VRF can be associated to multiple pools.
- DHCP server supports VRF by binding the address pool and the VLAN interface (which is connected to the DHCP client) to the same VRF.

Example

- Assign a DHCP address pool to a VRF.

```
admin@Xorplus# set protocols dhcp server pool pool2 vrf vrf1
admin@Xorplus# commit
```

set protocols dhcp server pool tftp-server

The **set protocols dhcp server pool tftp-server** command configures an IP address for the TFTP server that will be obtained by the DHCP client.

The **delete protocols dhcp server pool tftp-server** command deletes the configuration.

Command Syntax

set protocols dhcp server pool <*pool-name*> **tftp-server** <*tftp-server-ip*>

delete protocols dhcp [**server pool** <*pool-name*>] [**tftp-server**]

Parameters

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, and spaces are not supported.
tftp-server <*ipv4-address*>	Specifies the IPv4 address for the TFTP server address. The value is in dotted decimal notation. After the client sends request packets to the DHCP server, the TFTP server with this IP address will be replied.

Example

- Configure the IPv4 address 10.3.10.1 for the TFTP server.

```
admin@PICOS# set protocols dhcp server pool pool1 tftp-server 10.3.10.1
admin@PICOS# commit
```

set protocols dhcp server pool log-server

The **set protocols dhcp server pool log-server** command configures an IP address for the Syslog server that can be obtained by the DHCP client.

The **delete protocols dhcp server pool log-server** command deletes the configuration.

Command Syntax

set protocols dhcp server pool <*pool-name*> **log-server** <*log-server-ip*>

delete protocols dhcp [**server pool** <*pool-name*>] [**log-server**]

Parameters

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
log-server <*log-server-ip*>	Specifies the IP address for the Syslog server address. The value is in dotted decimal notation. After the client sends request packets to the DHCP server, the Syslog server with this IP address will be replied.

Example

- Configure the IP address 10.3.10.1 for the Syslog server.

```
admin@PICOS# set protocols dhcp server pool pool1 log-server 10.3.10.1
admin@PICOS# commit
```

set protocols dhcp server pool bootfile-name

The **set protocols dhcp server pool bootfile-name** command configures the file name with path or URL that can be obtained by the DHCP client.

The **delete protocols dhcp server pool bootfile-name** command deletes the configuration.

Command Syntax

set protocols dhcp server pool <*pool-name*> **bootfile-name** {**file-path** <*file-path*> | **url** <*url*>}

delete protocols dhcp server [**pool** <*pool-name*>][**bootfile-name**] [**file-path** | **url**]

Parameters

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
file-path <*file-path*>	Specifies the file name in the working path of the TFTP server. For example: *provision.sh.*
url <*url*>	Specifies the file name with URL on the HTTP server. For example: *http://192.168.1.1/provision.sh* You can only configure one of the path or URL, or the error prompt will appear.

Example

- Configure the file name with URL as http://192.168.1.1/provision.sh for the HTTP server.

```
admin@PICOS# set protocols dhcp server pool pool3 bootfile-name url http://192.168.1.1/provision.sh
admin@PICOS# commit
```

run show dhcp server binding address

The **run show dhcp server binding address** command shows the allocated IP address binding information.

Command Syntax

run show dhcp server binding [**vrf** <*vrf-name*>] [**address <***ipv4-address***>**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>]. Note that: The command shows the allocated IP address binding information in the default VRF if not explicitly specify a VRF name.
address <*ipv4-address***>**	Optional. Specifies an allocated address. The value is in dotted decimal notation.

Example

- View the allocated IP address binding information.

```
admin@Xorplus# run show dhcp server binding
2 bound clients

IP address      MAC address          Server      Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1    vlan100
10.1.1.88       00:0a:12:00:12:34    10.1.1.1    vlan100

admin@Xorplus# run show dhcp server binding vrf vrf1
1 bound clients

IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100

admin@Xorplus# run show dhcp server binding address 10.1.1.89
IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100

admin@Xorplus# run show dhcp server binding vrf vrf1 address 10.1.1.89
IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100
```

In the show result, "**Server**" represents the IP address of the Layer 3 VLAN interface connected to the DHCP client.

run show dhcp server binding interface

The **run show dhcp server binding interface** command displays the allocated IP address binding information based on the VLAN interface and configuration information of other parameters, including DNS server, domain name and default router.

Command Syntax

run show dhcp server binding interface {**all |** <*interface-name*>}

Parameter

Parameter	Description
interface {**all |** <*interface-name*>}	Specifies an L3 VLAN interface name. The value could be **all** or a specific VLAN interface name, where **all** indicates to show DHCP client information of all the VLAN interfaces.

Example

- View the allocated IP address binding information based on the VLAN interface.

```
admin@Xorplus# run show dhcp server binding interface vlan100
2 bound clients

Client Interface: vlan100

    MAC address:          00:0a:12:00:12:11
    Client IP Address:      10.1.1.88

    MAC address:          00:0a:12:00:12:12
    Client IP Address:      10.1.1.89

    DHCP Options :
    Name: dhcp-lease-time, Value: 43200 minutes
    Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3 ]
    Name: server-identifier, Value: 10.1.1.1
    Name: router, Value: [ 10.1.1.1 ]
    Name: domain-name, Value: example-50
```

Table 1. Description of the run show dhcp server binding interface command output

Item	Description
MAC address	Indicates the MAC address of a DHCP client.
Client IP Address	Indicates the IP address of a DHCP client.
Name: dhcp-lease-time	Indicates the lease time of the IP addresses.
Name: name-server	Indicates the IP address of the DNS server.
Name: server-identifier	Indicates the IP address of Layer 3 VLAN interface connected to the DHCP client.
Name: router	Indicates the default gateway for the DHCP clients.
Name: domain-name	Indicates the domain name for the DHCP clients.

set protocols dhcp server interface disable

In a direct connection scenario between the client and server, this command does not need to be configured.
In a non-direct connection scenario between the client and server, this command must be configured.

The **set protocols dhcp server interface disable** command enables DHCP server on the Layer 3 interface.

The **delete protocols dhcp server interface disable** command deletes the configuration.

Command Syntax

set protocols dhcp server interface <*interface-name*> **disable** <**true** | **false**>

delete protocols dhcp server interface <*interface-name*> **disable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
disable <**true**	**false**>	Enables or disables DHCP server on the Layer 3 interface. The value could be **true** or **false**. • **true**: Enables DHCP server on the Layer 3 interface. • **False**: Disables DHCP server on the Layer 3 interface. The default value is **False**.

Example

- Enable DHCP server on VLAN interface vlan10.

```
admin@PICOS# set protocols dhcp server interface vlan10 disable false
admin@PICOS# commit
```

set protocols dhcp6 relay interface disable

The **set protocols dhcp6 relay interface disable** command enables or disables DHCPv6 relay on a specified L3 interface.

Command Syntax

set protocols dhcp6 relay interface *<l3-interface-name>* **disable <true | false>**

Parameters

Parameter	Description
interface *<l3-interface-name>*	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <**true** | **false**>	Enables or disables DHCPv6 relay on an L3 interface, the value could be **true** or **false**: • **true**: Disables DHCPv6 relay. • **false**: Enables DHCPv6 relay. By default, DHCPv6 relay is disabled.

Usage Guidelines

Generally, DHCPv6 relay should be enabled on the L3 interface that connects to the host's network.

Example

- Enable DHCPv6 relay on the L3 VLAN interface vlan100.

```
admin@Switch# set protocols dhcp6 relay interface vlan100 disable false
admin@Switch# commit
```

set protocols dhcp6 relay interface destination

The **set protocols dhcp6 relay interface destination** command configures the IPv6 address of the DHCPv6 server or next-hop relay agent on the L3 interface enabled with DHCPv6 relay. You can repeat this command to configure multiple DHCPv6 servers.

Command Syntax

set protocols dhcp6 relay interface <*l3-interface-name*> **destination** <*ipv6-address*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
destination <*ipv6-address*>	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Example

- Configure the IPv6 address of the DHCPv6 server or next-hop relay agent on interface vlan100.

```
admin@Xorplus# set protocols dhcp6 relay interface vlan100 destination 205:147::205
admin@Xorplus# commit
```

set protocols dhcp6 relay interface remote-id

The **set protocols dhcp6 relay interface remote-id** command configures the remote ID to be inserted into the DHCPv6 relay packets.

Command Syntax

set protocols dhcp6 relay interface <*l3-interface-name*> **remote-id** <*remote-id*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. Its the outbound interface of relay messages.
remote-id <*remote-id*>	Specifies the remote ID. The value is a string.

Usage Guidelines

The Remote ID records user access information in the DHCPv6 packets sent from the clients to the device. When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the DHCPv6 relay can insert the Remote ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters.

Example

- Configure the remote ID to be inserted into the DHCPv6 relay packets.

```
admin@Xorplus# set protocols dhcp6 relay interface vlan100 remote-id ubuntuDesktop16.04.6-2
admin@Xorplus# commit
```

run show dhcp6 relay-stats

The **run show dhcp6 relay-stats** command displays DHCPv6 relay running status and statistics.

Command Syntax

run show dhcp6 relay-stats

Parameter

None.

Example

- Display DHCPv6 relay running status and statistics.

```
admin@Xorplus# run show dhcp6 relay-stats
Vif Name        Rx        Tx
-------------------------------------
vlan10          6866      1626
vlan20          2455      896
Total 2 Vif(s) enabled with DHCP6 relay
```

set protocols lacp interface rate

The **set protocols lacp interface rate** command configures the fast rate at which the peer switch interface sends LACP PDUs.

Command Syntax

set protocols lacp interface <*interface-name*> **rate** <**fast | slow** >

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name of the switch.
rate <**fast	slow** >	Specifies the rate at which the peer switch interface sends LACP PDUs. The value could be **fast** or **slow**. • When configuring the rate to **fast** mode, the period of sending LACP PDUs from the peer member interface is 1 second. If local member interface does not receive LACP PDU from the peer interface within 3 seconds (3 times the sending rate), the peer member interface will be considered unreachable and the status of the local member interface will be changed to Down immediately, and no more data will be forwarded through this interface. • When configuring the rate to **slow** mode, the period of sending LACP PDUs from the peer member interface is 30 seconds. The timeout of changing local interface status to Down is 90 seconds. The default rate mode is **slow**.

Example

- Enable LACP fast rate on interface xe-1/1/1.

```
admin@Xorplus# set protocols lacp interface xe-1/1/1 rate fast
admin@Xorplus# commit
```

run show lldp neighbor

The **run show lldp neighbor** command displays the neighbor device information of a specified interface or all the interfaces enabled LLDP.

Command Syntax

run show lldp neighbor [*<interface-name>* | **all**] [**detail**]

Parameter

Parameter	Description
[*<interface-name>* | **all**]	Optional. Specifies an interface name or **all**. **all** indicates to show the neighbor device information of all the interfaces enabled LLDP. If not specified, it will show the neighbor device information of all the interfaces enabled LLDP.
detail	Optional. Show details of the neighbor device information. If not specified, it will show the brief information of the neighbor device.

Example

- Display the details of neighbor device information of all the interfaces enabled LLDP.

```
admin@XorPlus# run show lldp neighbor all detail
Local Port: te-1/1/1
LLDP info:
------------------------------------------------------------------------------
  Time To Live: 106
  Chassis Id: 68:21:5F:7F:10:C6
  Port ID: te-1/1/1
  Port Description: te-1/1/1
  System Name: PICOS
  System Description: Pica8, Inc.,AS5835_54T, PICOS 4.3.2/9b1219e332
  System Capability: B, RBridge, Router
  System Enabled Capability: Bridge, Router
  Management Address: 10.10.51.12
  Default VLAN ID: 1
  Auto Negotiation: Supported, Enabled
  Physical media capabilities: Others, 10base_T, 100base_TX, 100base_TXFD, 1000base_T, 1000base_TFD
  Media Attachment Unit type: 1000base_T_Full_Duplex
  802.3 Power via MDI :Not available

LLDP MED is not Enabled.

Total entries displayed: 1
```

set protocols dhcp6 snooping vlan

The **set protocols dhcp6 snooping vlan disable** command enables DHCPv6 snooping in a specified VLAN.

Command Syntax

set protocols dhcp6 snooping vlan <*vlan-id*> **disable** <**true** | **false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true** | **false**>	Enables or disables DHCPv6 snooping, the value could be **true** or **false**: • **true**: Disables DHCPv6 snooping. • **false**: Enables DHCPv6 snooping. By default, DHCPv6 snooping is disabled.

Usage Guidelines

DHCPv6 snooping should be enabled in the VLAN, it takes effect only on the DHCPv6 messages received from the VLAN enabled with DHCPv6 snooping function. Packets received from the VLANs with DHCPv6 snooping disabled will not be processed by the DHCPv6 snooping module, and they will be processed and forwarded by the device as ordinary packets.

NOTE:

- The DHCPv6 snooping function is only practicable to the clients directly connected to the local L2 domain, rather than connected through a router.
- When DHCPv6 snooping is disabled, the DHCPv6 binding entry for the VLAN will be removed correspondingly.

Example

- Enable DHCPv6 snooping in VLAN 12.

```
admin@Xorplus# set protocols dhcp6 snooping vlan 12 disable false
admin@Xorplus# commit
```

set protocols dhcp6 snooping trust-port

The **set protocols dhcp6 snooping trust-port** command configures an interface as a trust interface for DHCPv6 snooping.

Command Syntax

set protocols dhcp6 snooping trust-port *<interface-name>*

Parameters

Parameter	Description
trust-port *<interface-name>*	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces.

Usage Guidelines

In order to make the DHCPv6 client obtain an IP address from a legitimate DHCPv6 server, the device interface directly or indirectly connected to the DHCPv6 server trusted by the administrator must be set to the trust interface, so as to prevent a spoofing DHCPv6 server from assigning an IP address to the DHCPv6 client.

The trusted interface forwards DHCPv6 packets received from the DHCPv6 server normally, whereas the untrusted interface discards DHCPv6 packets received from the DHCPv6 server.

Example

- Configure ge-1/1/1 as trust port for DHCPv6 snooping.

```
admin@Xorplus# set protocols dhcp6 snooping trust-port ge-/1/1/1
admin@Xorplus# commit
```

set protocols dhcp6 snooping binding file

The **set protocols dhcp6 snooping binding file** command configures a DHCPv6 snooping binding file for synchronizing DHCPv6 snooping entries from memory.

Command Syntax

set protocols dhcp6 snooping binding file <*file-path*>

Parameters

Parameter	Description
file <*file-path*>	Specifies a file path to save the DHCPv6 snooping binding table.

Usage Guidelines

If a DHCPv6 snooping binding file is specified, the DHCPv6 snooping entries will be synchronized from the memory to the binding file. This prevents DHCPv6 snooping entries data loss in case of power failure. By setting a DHCPv6 snooping binding file, the system can directly load the existing snooping entries from the binding file after if recovers.

For non-X86 devices, the path of the binding file is **/mnt/open/dhcp6_bind**; for X86 devices, the binding file path should not be under **/tmp**.

Example

- Configure the DHCPv6 snooping binding file.

```
admin@Xorplus# set protocols dhcp6 snooping binding file /mnt/open/dhcp6_bind
admin@XorPlus# commit
```

set protocols dhcp6 snooping binding write-delay

The **set protocols dhcp6 snooping binding write-delay** command configures a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

Command Syntax

set protocols dhcp6 snooping binding write-delay <*write-delay-timer*>

Parameters

Parameter	Description
write-delay <*write-delay-timer*>	Specifies a delay timer for writing the DHCPv6 snooping entries from the memory to the binding file. The value is an integer in seconds that ranges from 15 to 86400. The default value is 300s.

Usage Guidelines

In order to reduce the system burden caused by frequent file writes, you can configure a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

NOTE:

In the case when the DHCPv6 snooping entry is changed by the administrator configuration modifications from the CLI, such as modifying the VLAN, the binding file will be immediately refreshed rather than wait for write-delay timer.

Example

- Configure a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

```
admin@Xorplus# set protocols dhcp6 snooping binding write-delay 24
admin@XorPlus# commit
```

set protocols dhcp6 snooping vlan option-policy

The **set protocols dhcp6 snooping vlan option-policy** command configures how to handle the Option field when receiving a DHCPv6 message on VLANs where DHCPv6 snooping is enabled.

Command Syntax

set protocols dhcp6 snooping vlan <*vlan-id*> **option-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
option-policy <**drop	keep	insert	replace>**	Specifies the policy for Option. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 18 or Option 37 field. If the received DHCPv6 packets without Option 18 or Option 37 values, the packets will be forwarded. • **keep**: Option 18 and Option 37 in the packet remain unchanged and forwarded. • **insert**: the existing Option 18 or Option 37 remain unchanged; else, insert Option 18 or Option 37 with the value the administrator configured if not exist, then forwarding the packet to the DHCP server. • **replace**: The existing Option 18 and Option 37 will be replaced with the value administrator configured, then forwarded; Else, if not exist, the system inserts Option 18 or Option 37 with the value the administrator configured . The default value is **keep**.

Usage Guidelines

Option policy is used when receiving a DHCPv6 message from the DHCPv6 client. When option policy is set to “insert” or “replace”, you can use the following commands to set the format of interface ID and remote ID sub-options:

set protocols dhcp6 snooping option18 interface-id <port-index | port-name | port-description>
set protocols dhcp6 snooping option37 remote-id <*remote-id*>

Example

- Configure the Option policy.

```
admin@Xorplus# set protocols dhcp6 snooping vlan 12 option-policy insert
admin@Xorplus# commit
```

set protocols dhcp6 snooping option37 remote-id

The **set protocols dhcp6 snooping option37 remote-id** command configures the format of sub-option remote ID inserted into the Option 37 field for DHCPv6 snooping.

NOTE: The sub-option remote ID is applied to VLANs where option-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp6 snooping option37 remote-id <*remote-id*>

Parameters

Parameter	Description
remote-id <*remote-id*>	Specifies the type of remote ID in the Option 37 field. The value is a string. By default, the sub-option remote ID is not configured which means remote ID is not enabled.

Usage Guidelines

If configured, the remote-id field may be used to encode, for instance:

o a "caller ID" telephone number for dial-up connection
o a "user name" prompted for by a Remote Access Server
o a remote caller ATM address
o a "modem ID" of a cable data modem
o the remote IP address of a point-to-point link
o a remote X.25 address for X.25 connections
o an interface or port identifier

Example

- Configure the type of sub-option remote ID inserted into the DHCPv6 Option 37 field.

```
admin@Xorplus# set protocols dhcp6 snooping option37 remote-id Xorplus
admin@Xorplus# commit
```

set protocols dhcp6 snooping option18 interface-id

The **set protocols dhcp6 snooping option18 interface-id** command configures the format of sub-option interface ID inserted into the Option 18 field for DHCPv6 snooping.

NOTE: The sub-option interface ID is applied to VLANs where option-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp6 snooping option18 interface-id <port-index | port-name | port-description>

Parameters

Parameter	Description
interface-id <port-index | port-name | port-description>	Specifies the type of interface ID in the Option 18 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option interface ID is not configured which means interface ID is not enabled.

Usage Guidelines

If configured, the interface ID is filled with the port identifier and VLAN.

- When “port-index” is selected, the format of the interface ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the interface ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the interface ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernet *<lag_name>* **description** *<description>*

set interface gigabit-ethernet *<physical-port>* **description** *<description>*

Example

- Configure the format of the sub-option interface ID for the Option 18 field.

```
admin@Xorplus# set protocols dhcp6 snooping option18 interface-id port-index
admin@Xorplus# commit
```

set protocols dhcp6 snooping interface max-clients

The **set protocols dhcp6 snooping interface max-clients** command configures the maximum number of supported DHCPv6 clients accessed to physical port according to network status.

> When the number of clients in the DHCPv6 snooping binding table reaches this maximum value on this interface, any exceeding DHCPv6 packets will be discarded.

Command Syntax

set protocols dhcp6 snooping interface <*interface-name*> **max-clients** <*max-number*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port.
max-clients <*max-number*>	Specifies maximum number of supported users. The value is an integer that ranges from 1 to 2048. The default value is 1024.

Example

- Configure the maximum number of supported DHCPv6 clients accessed to physical port according to network status.

```
admin@Xorplus# set protocols dhcp6 snooping interface ge-1/1/1 max-clients 2000
admin@Xorplus# commit
```

run show dhcp6 snooping binding

The **run show dhcp6 snooping binding** command displays the DHCPv6 snooping binding table, which includes the user MAC address, IP address, VLAN ID, access interface and the lease time.

Command Syntax

run show dhcp6 snooping binding

Parameter

None.

Example

- Show the DHCPv6 snooping binding table.

```
admin@Xorplus# run show dhcp6 snooping binding
Total count:     2
MAC Address     IPv6 Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------
e4:f0:04:89:b6:46  0        ae65            1         0/0
14:18:77:18:2c:b9   2::1       ae25            125       599/600
```

Table 1. Description of the run show dhcpv6 snooping binding command output

Item	Description
Mac Address	User MAC address.
IPv6 Address	User IPv6 address.
Port	User access interface.
VLAN ID	User VLAN ID.
Lease(sec)	Lease time for the IP address, in seconds. The format displayed is **Remaining Lease Time/Total Lease Time**.

set protocols dhcp6 guard policy device-role

The **set protocols dhcp6 guard policy device-role** command can set the device role to client or server.

The **delete protocols dhcp6 guard policy device-role** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy *<policy-name>* **device-role <server | client>**

delete protocols dhcp6 guard policy *<policy-name>* **device-role**

Parameter

Parameter	Description
policy *<policy-name>*	Specifies the guard policy. The value is a policy name.
device-role <server | client>	Set the device role to client or server. The value could be **server** or **client**. **sever**: Set the device role to server. **client**: Set the device role to client. By default, the device role is **client**.

Example

- Set the device role of guard policy p1 to server.

```
admin@PICOS# set protocols dhcp6 guard policy p1 device-role server
admin@PICOS# commit
```

set protocols dhcp6 guard policy trust-port

The **set protocols dhcp6 guard policy trust-port** command can set the guard policy to trust port.

The **delete protocols dhcp6 guard policy trust-port** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **trust-port**

delete protocols dhcp6 guard policy <*policy-name*> **trust-port**

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.

Example

- Set the guard policy p1 to trust port.

```
admin@PICOS# set protocols dhcp6 guard policy p1 trust-port
admin@PICOS# commit
```

set protocols dhcp6 guard policy interface

The **set protocols dhcp6 guard policy interface** command can configure guard policy on an interface.

The **delete protocols dhcp6 guard policy interface** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **interface** <*interface-name*>

delete protocols dhcp6 guard policy <*policy-name*> **interface** <*interface-name*>

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
interface <*interface-name*>	Specifies the interface name. The value is a physical port or an LAG port.

Example

- Configure guard policy p1 on interface ge-1/1/2.

```
admin@PICOS# set protocols dhcp6 guard policy p1 interface ge-1/1/2
admin@PICOS# commit
```

set protocols dhcp6 guard policy preference-min

The **set protocols dhcp6 guard policy preference-min** command can set the minimum preference value for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy preference-min** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy *<policy-name>* **preference-min** *<min-value>*

delete protocols dhcp6 guard policy *<policy-name>* **preference-min**

Parameters

Parameter	Description
policy *<policy-name>*	Specifies the guard policy. The value is a policy name.
preference-min *<min-value>*	Specifies the minimum preference value. The value is an integer that ranges from 0 to 255. By default, the minimum preference value is 0.

Example

- Set the minimum preference value of guard policy p1 to 10.

```
admin@PICOS# set protocols dhcp6 guard policy p1 preference-min 10
admin@PICOS# commit
```

set protocols dhcp6 guard policy preference-max

The **set protocols dhcp6 guard policy preference-max** command can set the maximum preference value for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy preference-max** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **preference-max** <*max-value*>

delete protocols dhcp6 guard policy <*policy-name*> **preference-max**

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
preference-max <*max-value*>	Specifies the maximum preference value. The value is an integer that ranges from 0 to 255. By default, the maximum preference value is 255.

Example

- Set the maximum preference value of guard policy p1 to 200.

```
admin@PICOS# set protocols dhcp6 guard policy p1 preference-max 200
admin@PICOS# commit
```

set protocols dhcp6 guard policy match server source-address

The **set protocols dhcp6 guard policy match server source-address** command can set the server source-address for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy match server source-address** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy *<policy-name>* **match server source-address** *<IPv6Net>*

delete protocols dhcp6 guard policy *<policy-name>* **match server source-address** *<IPv6Net>*

Parameters

Parameter	Description
policy *<policy-name>*	Specifies the guard policy. The value is a policy name.
source-address *<IPv6Net>*	Specifies the server source-address. The value is an IPv6 address.

Example

- Set the server source-address of guard policy p1 to 2001::1/128.

```
admin@PICOS# set protocols dhcp6 guard policy p1 match server source-address 2001::1/128
admin@PICOS# commit
```

set protocols dhcp6 guard policy match reply ia-prefix

The **set protocols dhcp6 guard policy match reply ia-prefix** command can set the ia-prefix for Reply packets to allow forwarding.

The **delete protocols dhcp6 guard policy match reply ia-prefix** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **match reply ia-prefix** <*IPv6Net*>

delete protocols dhcp6 guard policy <*policy-name*> **match reply ia-prefix** <*IPv6Net*>

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
ia-prefix <*IPv6Net*>	Specifies the ia-prefix. The value is an IPv6 address.

Example

- Set the ia-prefix for Reply packets of guard policy p1 to 3001::0/64.

```
admin@PICOS# set protocols dhcp6 guard policy p1 match reply ia-prefix 3001::0/64
admin@PICOS# commit
```

run show dhcp6 guard policy

The **run show dhcp6 guard policy** command shows the information of the dhcp6 guard policy configuration.

Command Syntax

run show dhcp6 guard policy <*policy-name*>

Parameter

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.

Example

- View the information of the dhcp6 guard policy configuration.

```
admin@PICOS# run show dhcp6 guard policy p1
dhcp6 guard policy: p1
    match:
        server source-address: 2001::/64
              reply ia-prefix: 3001::/64
    preference-max: 255
    preference-min: 0
    device role: server
    interface: ge-1/1/1
```

run show dhcp6 guard

The **run show dhcp6 guard** command shows the information of the dhcp6 guard configuration.

Command Syntax

run show dhcp6 guard

Parameter

None.

Example

- View the information of the dhcp6 guard configuration.

```
admin@PICOS# run show dhcp6 guard
dhcp6 guard policy: p1
    match:
        server source-address: 2001::/64
              reply ia-prefix: 3001::/64
    preference-max: 255
    preference-min: 0
    device role: server
    interface: ge-1/1/1
dhcp6 guard policy: p2
    device role: client
    interface: ge-1/1/2
```

run show arp

The **run show arp** command is used to view IPv4 ARP entries.

Command Syntax

run show arp [**vrf** <*vrf-name*> | **brief** | **management-ethernet | statistics**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. When a VRF is specified, only the IPv4 ARP entries of the specific VRF are displayed. When no VRF is specified, the result shows only the IPv4 ARP entries of the default VRF.
brief	Optional. View the brief information of ARP entries.
management-ethernet	Optional. View the ARP entry of management interface.
statistics	Optional. View the statistics of ARP communication packets.

Example

- View all IPv4 ARP entries.

```
admin@PICOS# run show arp
Aging-time(seconds): 1200
Total count        : 1
Address      HW Address       Type     Interface  Age
---------------  -----------------      -------     ---------   -----
20.20.20.3   70:72:CF:9D:6F:FB  Dynamic  vlan20    591
```

- View the brief information of ARP entries.

```
admin@PICOS# run show arp brief
Aging-time(seconds): 1200
Total count        : 1
```

- View the ARP entry of management interface.

```
admin@PICOS# run show arp management-ethernet
Address          HW Address         Interface
---------------  -----------------  ---------
```

- View the statistics of ARP communication packets.

```
admin@PICOS# run show arp statistics
ARP statistics:
```

```
Recv: 0 requests (0 gratuitous), 0 replies
Sent: 0 requests (0 gratuitous), 0 replies
Resolve requests rcvd: 0
Resolve requests dropped: 0
```

set protocols sflow interface polling-interval

Users can set the polling interval for a specified interface.

Command Syntax

set protocols sflow interface <*port*> **polling-interval** <*seconds*>

***d*elete protocols sflow interface** <*port*> **polling-interval**

Parameter

Parameter	Description
interface <*port*>	Ethernet switching port identifier,the valid ports range 1-52.
polling-interval <*seconds*>	Number of seconds, [0..3600]

Example

• This example is to set polling interval to 300 on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 polling-interval 300
admin@XorPlus# commit
```

set protocols sflow header-len

Users can set the length of sampled packet in bytes.

Command Syntax
set protocols sflow header-len *<len>*
delete protocols sflow header-len

Parameter

Parameter	Description
header-len *<len>*	The Length of sampled packet in bytes

Example
• This example is to set length of sampled packet to 1024:

```
admin@XorPlus# set protocols sflow header-len 1024
admin@XorPlus# commit
```

set protocols sflow interface header-len

Users can set the Length of sampled packet in bytes.

Command Syntax
set protocols sflow interface <*port*> **header-len** <*value*>
delete protocols sflow interface <*port*> **header-len**

Parameters

Parameter	Description
interface <*port*>	Ethernet switching port identifier,the valid ports range 1-52
header-len <*value*>	The length identifier, [14..9216]

Example
• This example is to set header length sampled packets to 15 on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 header-len 15
admin@XorPlus#
```

set protocols sflow interfac sampling-rate egress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow interface <*port*> **sampling-rate egress** <*value*>
delete protocols sflow interface <*port*> **sampling-rate egress**

Parameters

Parameter	Description
interface <*port*>	Ethernet switching port identifier,the valid ports range 1-52.
egress <*value*>	The rate at which exiting packets must be sampled, 2000 by default,[0..1048576].

Example
• This example is to set sampling rate of egress to 1000:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 sampling-rate egress 1000
admin@XorPlus# commit
```

set protocols sflow interface disable

Users can configure a specified interface to sflow protocol.

Command Syntax
set protocols sflow interface <*port*> **disable** <*bool*>
delete protocols sflow interface <*port*> **disable**

Parameter

Parameter	Description
interface <*port*>	ethernet switching port identifier,the valid ports range 1-52.
<*bool*>	Disable or enable sflow on a specified interface. • **true**: disables sflow on a specified interface • **false**: enables sflow on a specified interface

Example
• This example is to enable sflow on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 disable false
admin@XorPlus# commit
```

set protocols sflow interface sampling-rate ingress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow interface <*port*> **sampling-rate ingress** <*value*>
delete protocols sflow interface <*port*> **sampling-rate ingress**

Parameter

Parameter	Description
interface <*port*>	Ethernet switching port identifier,the valid ports range 1-52.
ingress <*value*>	The rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example

• This example is to set sampling rate of ingress to 1000:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 sampling-rate ingress 1000
admin@XorPlus# commit
```

set protocols sflow polling-interval

Users can set polling interval the sflow agent polls interfaces in seconds.

Command Syntax

set protocols sflow polling-interval <*time*>

Parameter

Parameter	Description
polling-interval <*time*>	Number of seconds, how often the sflow agent polls interfaces in seconds, 30 by default.

Example

• This example is to set polling interval to 60:

```
admin@XorPlus# set protocols sflow polling-interval 60
admin@XorPlus# commit
```

set protocols sflow sampling-rate egress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow sampling-rate egress <*value*>
delete protocols sflow sampling-rate egress

Parameter

Parameter	Description
egress <*value*>	The rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example
• This example is to set sampling rate of egress to 1000:

```
admin@XorPlus# set protocols sflow sampling-rate egress 1000
admin@XorPlus# commit
```

set protocols sflow sampling-rate ingress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow sampling-rate ingress <*value*>
delete protocols sflow sampling-rate ingress

Parameter

Parameter	Description
ingress <*value*>	The rate at which exiting packets must be sampled, 2000 by default,[0..1048576].

Example
• This example is to set sampling rate of ingress to 1000:

```
admin@XorPlus# set protocols sflow sampling-rate ingress 1000
admin@XorPlus# commit
```

set protocols sflow source-address

Users can set the source address as the source in packets transmitted to collectors.

Command Syntax

set protocols sflow source-address *<IPv4>*

Parameter

Parameter	Description
source-address *<IPv4>*	Source address as the source in packets transmitted to collectors

Example

• This example is to set source-address to 10.10.50.248:

```
admin@XorPlus# set protocols sflow source-address 10.10.50.248
admin@XorPlus# commit
```

IP Multicast Commands

- IGMP Snooping Configuration Commands
  - run show igmp-snooping
  - run show igmp-snooping groups
  - run show igmp-snooping mrouter
  - run show igmp-snooping querier
  - set protocols igmp-snooping enable
  - set protocols igmp-snooping interface max-groups
  - set protocols igmp-snooping last-member-query-count
  - set protocols igmp-snooping last-member-query-interval
  - set protocols igmp-snooping max-response-time
  - set protocols igmp-snooping query-interval
  - set protocols igmp-snooping report-suppression
  - set protocols igmp-snooping robustness-variable
  - set protocols igmp-snooping vlan-id enable
  - set protocols igmp-snooping vlan-id fast-leave
  - set protocols igmp-snooping vlan-id mrouter interface
  - set protocols igmp-snooping vlan-id querier address
  - set protocols igmp-snooping vlan-id querier enable
  - set protocols igmp-snooping vlan-id querier other-querier-timer
  - set protocols igmp-snooping vlan-id querier version
  - set protocols igmp-snooping vlan-id static group interface
  - set protocols igmp-snooping vlan-id unregistered flood-all
- IGMP Commands
  - set protocols igmp interface
  - set protocols igmp interface join-group
  - set protocols igmp interface query-interval
  - set protocols igmp interface query-max-response-time
  - set protocols igmp interface version
  - run show igmp groups
  - run show igmp interface
- PIM Configuration Commands
  - set protocols pim ecmp
  - set protocols pim interface active-active
  - set protocols pim interface drpriority
  - set protocols pim interface hello holdtime
  - set protocols pim interface hello interval
  - set protocols pim interface sm
  - set protocols pim interface use-source
  - set protocols pim join-prune-interval
  - set protocols pim keep-alive-timer
  - set protocols pim packets
  - set protocols pim register-suppress-time
  - set protocols pim rp
  - set protocols pim spt-switchover infinity-and-beyond
  - set protocols pim ssm prefix-list
  - set protocols pim interface bsm
  - set protocols pim interface unicast-bsm
  - run show pim interface
  - run show pim rp-info
  - run show pim neighbor
  - run show pim upstream
  - run show mroute
  - mtrace
  - run show pim group-type
  - run show pim bsr
  - run show pim bsm-database
  - run show pim bsrp-info
  - run clear pim bsr-data
- Multicast Source Discovery Protocol (MSDP) Commands
  - set protocols msdp mesh-group source
  - set protocols msdp mesh-group member
  - run show msdp mesh-group
  - run show msdp peer
  - run show msdp sa
- Multicast VLAN Registration (MVR) Commands

- run show igmp-snooping mvr mvlan
- run show igmp-snooping mvr receiver-vlan
- set protocols igmp-snooping vlan-id mvr receiver vlan-list
- set protocols igmp-snooping vlan-id mvr source group

IGMP Snooping Configuration Commands

- run show igmp-snooping
- run show igmp-snooping groups
- run show igmp-snooping mrouter
- run show igmp-snooping querier
- set protocols igmp-snooping enable
- set protocols igmp-snooping interface max-groups
- set protocols igmp-snooping last-member-query-count
- set protocols igmp-snooping last-member-query-interval
- set protocols igmp-snooping max-response-time
- set protocols igmp-snooping query-interval
- set protocols igmp-snooping report-suppression
- set protocols igmp-snooping robustness-variable
- set protocols igmp-snooping vlan-id enable
- set protocols igmp-snooping vlan-id fast-leave
- set protocols igmp-snooping vlan-id mrouter interface
- set protocols igmp-snooping vlan-id querier address
- set protocols igmp-snooping vlan-id querier enable
- set protocols igmp-snooping vlan-id querier other-querier-timer
- set protocols igmp-snooping vlan-id querier version
- set protocols igmp-snooping vlan-id static group interface
- set protocols igmp-snooping vlan-id unregistered flood-all

run show igmp-snooping

The **run show igmp-snooping** command shows the configuration information of IGMP snooping.

Command Syntax

run show igmp-snooping [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the configuration information of IGMP snooping.

```
admin@XorPlus# run show igmp-snooping
Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping             : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Router aging time            : 260
Max response time            : 10
Query interval               : 60
Last member query count      : 2
Last member query interval   : 2
```

- Show the IGMP snooping configuration of a specific VLAN.

```
admin@XorPlus# run show igmp-snooping vlan 1
Vlan 1:
----------------------------------------------
IGMP snooping                       : Enabled
IGMPv2 fast leave                   : Enabled
IGMP querier state                  : Enabled
IGMP querier source ip address      : 0.0.0.0
IGMP other querier timer            : 1
IGMP querier version                : 2
```

run show igmp-snooping groups

The **run show igmp-snooping groups** command shows information about multicast group member ports which is used for Layer 2 forwarding, namely, the Layer 2 forwarding table.

Command Syntax

run show igmp-snooping groups [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the information about multicast group member ports.

```
admin@XorPlus# run show igmp-snooping groups
Vlan      Group                   Port List          Type
--------  ------------------   -----------------   ----------------------
1         238.255.0.1             ge-1/1/2           Static
                                  ge-1/1/1           Mrouter
```

run show igmp-snooping mrouter

The **run show igmp-snooping mrouter** command shows the information about IGMP snooping router port.

Command Syntax

run show igmp-snooping mrouter [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the information about IGMP snooping router port.

```
admin@XorPlus# run show igmp-snooping mrouter
Vlan           Ports          Type
--------    -------------     ---------
1              ge-1/1/1       Static
```

run show igmp-snooping querier

The **run show igmp-snooping querier** command shows the configuration information and status of the querier in a VLAN.

Command Syntax

run show igmp-snooping querier [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the configuration information and status of the querier.

```
admin@XorPlus# run show igmp-snooping querier vlan 1
Vlan 1:   IGMP switch querier status
------------------------------------------------------------
admin state                    : Disabled
admin version                  : 2
source IP address              : 0.0.0.0
other querier timer            : 1
operational state              : Non-Querier
```

set protocols igmp-snooping enable

The **set protocols igmp-snooping enable** command is used to enable or disable the global IGMP snooping function.

Command Syntax

set protocols igmp-snooping enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the global IGMP snooping function. The value is **true** or **false**. • **true**: enables the global IGMP snooping function. • **false**: disables the global IGMP snooping function. The default value is **false**.

Usage Guidelines

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Example

- Enable the global IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping enable true
admin@Xorplus# commit
```

set protocols igmp-snooping interface max-groups

The **set protocols igmp-snooping interface max-groups** command configures the maximum number of static/dynamic multicast groups that a specific interface can join.

The **delete protocols igmp-snooping interface max-groups** command sets the maximum number of static/dynamic multicast groups on a specific interface to the default value of 256.

Command Syntax

set protocols igmp-snooping interface <*interface-name*> **max-groups** <*int*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value is a string.
max-groups <*int*>	Specifies the maximum number of static/dynamic multicast groups on a specific interface. The value is an integer. Range: 1 to 256. Default: 256.

Usage Guidelines

By configuring this command, users can control the maximum number of static/dynamic multicast groups on a specific interface. If the number of Layer 2 multicast entries on the interface already exceeds the configured limit, the number of Layer 2 multicast entries on the interface does not change and the interface cannot learn new Layer 2 multicast entries.

The Layer 2 multicast table can be viewed by using the command **run show igmp-snooping groups**.

If the multicast groups number of an interface has already reached the configured max number of multicast groups, the system will report an error under the following two conditions:

- The system prints a warning message in the syslog when receiving IGMP packets with new multicast groups, prompting that the number of multicast groups on the interface exceeding the configured max number of multicast groups. For example,

```
Nov 11 2022 09:48:13 PICOS  local0.warning : [IGMPSNOOPING]The number of groups (6) reaches to the configured maximum number (6) on
Nov 11 2022 09:48:14 PICOS  local0.warning : [IGMPSNOOPING]The number of groups (8) reaches to the configured maximum number (8) on
```

- Users cannot configure anymore new static multicast groups when the number of multicast groups on an interface has already reached the configured max number of multicast groups. Commit fails with an error message "Already reach max multicast mac entries count : *value of max-groups*". For example,

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 static group 224.1.2.2 interface te-1/1/23
admin@PICOS# commit
Already reach max multicast mac entries count : 256
Commit failed.
```

Example

- Configure the maximum number of static/dynamic multicast groups on interface te-1/1/24.

```
admin@PICOS# set protocols igmp-snooping interface te-1/1/24 max-groups 8
admin@PICOS# commit
```

set protocols igmp-snooping last-member-query-count

The **set protocols igmp-snooping last-member-query-count** command configures the number of times that the querier sends a group-specific query message.

Command Syntax

set protocols igmp-snooping last-member-query-count <*last-member-query-count*>

Parameter

Parameter	Description
last-member-query-count <*last-member-query-count*>	Specifies the number of times that the querier sends a group-specific query message. The value is an integer ranges from 1 to 7. The default value is 2.

Usage Guidelines

When the switch receives an IGMP leave message from a host, it sends the group-specific query messages to query whether the particular multicast group still has members and starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = last-member-query-count × last-member-query-interval **+** max-response-time. The **set protocols igmp-snooping last-member-query-count** command is used to configure the last-member-query-count in the above formula. The last-member-query-interval can be configured using the **set protocols igmp-snooping last-member-query-interval** command. The max-response-time can be configured using the **set protocols igmp-snooping max-response-time** command.

If the switch receives a report message from other hosts within the aging time, it continues to maintain memberships of the particular multicast group. However, if the switch receives no report message within the aging time, it will stop maintaining memberships of the particular multicast group and delete the particular multicast group entry in the Layer 2 forwarding table.

Example

- Configure the number of times that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-count 2
admin@Xorplus# commit
```

set protocols igmp-snooping last-member-query-interval

The **set protocols igmp-snooping last-member-query-interval** command configures the interval that the querier sends a group-specific query message.

Command Syntax

set protocols igmp-snooping last-member-query-interval <*last-member-query-interval*>

Parameter

Parameter	Description
last-member-query-interval <*last-member-query-interval*>	Specifies the interval of sending a particular multicast group query packet. The value is an integer, in seconds, that ranges from 1 to 32. The default value is 2.

Usage Guidelines

When the switch receives an IGMP leave message from a host, it sends the group-specific query messages to query whether the particular multicast group still has members and starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = last-member-query-count × last-member-query-interval **+** max-response-time. The **set protocols igmp-snooping last-member-query-count** command is used to configure the last-member-query-count in the above formula. The last-member-query-interval can be configured using the **set protocols igmp-snooping last-member-query-interval** command. The max-response-time can be configured using the **set protocols igmp-snooping max-response-time** command.

If the switch receives a report message from other hosts within the aging time, it continues to maintain memberships of the particular multicast group. If the switch receives no report message within the aging time, it will stop maintaining memberships of the particular multicast group and delete the particular multicast group entry in the Layer 2 forwarding table.

Example

- Configure the interval that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-interval 2
admin@XorPlus# commit
```

set protocols igmp-snooping max-response-time

The **set protocols igmp-snooping max-response-time** command configures the maximum response time for an IGMP general query message or a group-specific query message.

Command Syntax

set protocols igmp-snooping max-response-time <*max-response-time*>

Parameter

Parameter	Description
max-response-time <*max-response-time*>	Specifies the maximum response time for an IGMP general query message or a group-specific query message. The value is an integer, in seconds, that ranges from 1 to 25. The default value is 10.

Usage Guidelines

The maximum response time can be used to adjust the aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping max-response-time** command is used to configure the maximum response time in the above formula. The General query count can be configured using the **set protocols igmp-snooping robustness-variable** command. The General query interval can be configured using the **set protocols igmp-snooping query-interval** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

The maximum response time can be used to adjust the aging time of member ports when the switch receives an IGMP leave message from a host, for detail please refer to **set protocols igmp-snooping last-member-query-count** command.

NOTE:

- We recommend setting the value of **Maximum response time** smaller than the value of **General query interval**.
- The aging time takes effect only on dynamic member ports, however, the static member ports do not age.

Example

- Configure the maximum response time for IGMP general query message.

```
admin@Xorplus# set protocols igmp-snooping max-response-time 10
admin@XorPlus# commit
```

set protocols igmp-snooping query-interval

The **set protocols igmp-snooping query-interval** command configures the interval of sending IGMP general query message.

Command Syntax

set protocols igmp-snooping query-interval <*query-interval*>

Parameter

Parameter	Description
max-response-time <*max-response-time*>	Specifies the interval of sending an IGMP general query message. The value is an integer, in seconds, that ranges from 1 to 18000. The default value is 60.

Usage Guidelines

The query interval can be used to adjust aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping query-interval** command is used to configure the General query interval in the above formula. The General query count can be configured using the **set protocols igmp-snooping robustness-variable** command. The Maximum response time can be configured using the **set protocols igmp-snooping max-response-time** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

NOTE:

- We recommend setting the value of **Maximum response time** smaller than the value of **General query interval**.
- The aging time takes effect only on dynamic member ports, however, the static member ports do not age.

Example

- Configure the interval of sending IGMP general queries.

```
admin@Xorplus# set protocols igmp-snooping query-interval 60
admin@XorPlus# commit
```

set protocols igmp-snooping report-suppression

The **set protocols igmp-snooping report-suppression** command is used to enable or disable the IGMP snooping membership report suppression function.

Command Syntax

set protocols igmp-snooping report-suppression <**true | false**>

Parameter

Parameter	Description
report-suppression <**true	false**>	Enable or disable the membership report suppression function. The value is **true** or **false**. • **true**: enables the membership report suppression function. • **false**: disables the membership report suppression function. The default value is **false**.

Usage Guidelines

When IGMP snooping membership report suppression function is enabled, the Layer 2 device will forward only one IGMP report of a multicast group to the upstream device in suppression time of 1/2 of query time. The Layer 2 device will reset the suppression timer when receiving the first IGMP report message. Only when the first member joins a multicast group when a host sends a report message, the Layer 2 switch will forward the report message to the upstream device for creating or maintaining the multicast entry. This function helps to reduce the amount of IGMP snooping traffic in the network.

Example

- Enable the IGMP snooping membership report suppression function.

```
admin@Xorplus# set protocols igmp-snooping report-suppression true
admin@XorPlus# commit
```

set protocols igmp-snooping robustness-variable

The **set protocols igmp-snooping robustness-variable** command configures the IGMP robustness coefficient.

Command Syntax

set protocols igmp-snooping robustness-variable <*robustness-variable*>

Parameter

Parameter	Description
robustness-variable <*robustness-variable*>	Specifies the IGMP robustness coefficient. The value is an integer that ranges from 2 to 4. The default value is 2.

Usage Guidelines

The robustness coefficient can be used to adjust aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping robustness-variable** command is used to configure the General query count in the above formula. The General query interval can be configured using the **set protocols igmp-snooping query-interval** command. The Maximum response time can be configured using the **set protocols igmp-snooping max-response-time** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

NOTE:

The aging time takes effect only on dynamic member ports whereas static member ports do not age.

Example

- Configure the IGMP robustness coefficient.

```
admin@Xorplus# set protocols igmp-snooping robustness-variable 2
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id enable

The Internet Group Management Protocol (IGMP) is used to establish multicast group membership on IPv4 networks, making it an important component of IP multicast. It is used for one-to-many applications such as video streaming and gaming. IGMP snooping involves the process of listening for IGMP traffic between hosts and routers, enabling a switch to learn which devices are involved in which IP multicast conversations. This enables multicasts to be filtered from links and ports where they're not needed, thus reducing network traffic. IGMP snooping is typically disabled by default on network switches. This document details how to enable IGMP if desired, on a per-VLAN basis.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **enable** <**true** | **false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true** | **false**>	Enable or disable the VLAN-based IGMP snooping function. The value is **true** or **false**. • **true**: enables the VLAN-based IGMP snooping function. • **false**: disables the VLAN-based IGMP snooping function. The default value is **false**.

Usage Guidelines

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Example

- Enable the VLAN-based IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 enable true
admin@Xorplus# commit
```

set protocols igmp-snooping vlan-id fast-leave

The **set protocols igmp-snooping vlan-id fast-leave** command is used to enable or disable the fast leave function to allow member ports in a VLAN to quickly leave the multicast group.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **fast-leave** <**true | false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
fast-leave <**true	false**>	Enable or disable the fast leave function. The value is **true** or **false**. • **true**: enables the fast leave function. • **false**: disables the fast leave function. The default value is **false**.

Usage Guidelines

Fast leave of a member port means that the switch will delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP leave message for the group, instead of waiting for the member port to age.

> **NOTE:**
>
> When there are multiple receiver hosts under an interface, this function may interrupt other hosts in the same multicast group in receiving multicast data. So, it is recommended to disable the fast leave function in this scenario.

Example

- Enable the fast leave function to allow member ports in a VLAN to quickly leave the multicast groups.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 fast-leave true
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id mrouter interface

The **set protocols igmp-snooping vlan-id mrouter interface** command configures the interface as a static router port in the specified VLAN.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mrouter interface** <*interface-name*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies the interface of the switch as a static router port.

Usage Guidelines

If you need to forward IGMP report / leave packets from one interface to the upstream IGMP querier permanently and stably, you can configure the interface as a static router port. Static router port will not be affected by the aging time, it will not age.

Example

- Configure the interface as a static router port in the specified VLAN.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 mrouter interface ge-1/1/3
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier address

The **set protocols igmp-snooping vlan-id querier address** command configures the source IP address of the general query message and group-specific query message sent by the querier.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier address** <*querier-address*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
querier address <*querier-address*>	Specifies a source IP address. The value is in dotted decimal notation. The default value is 0.0.0.0.

Usage Guidelines

After the Layer 2 device enables the querier function, you can run this command to configure the source IP address of the general query message and group-specific query message sent by the querier.

Example

- Configure the source IP address of the general query message and group-specific query message sent by the querier.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier address 192.168.10.2
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier enable

The **set protocols igmp-snooping vlan-id querier enable** command is used to enable or disable the querier function in a VLAN.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier enable** <**true | false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true	false**>	Enable or disable the querier function in a VLAN. The value is **true** or **false**. • **true**: enables the querier function in a VLAN. • **false**: disables the querier function in a VLAN. The default value is **false**.

Usage Guidelines

When a Layer 3 multicast device is not running the IGMP protocol or in a pure Layer 2 network, IGMP snooping querier can be configured on a Layer 2 device to send IGMP query messages.

Example

- Enable the querier function in a VLAN.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier enable true
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier other-querier-timer

The **set protocols igmp-snooping vlan-id querier other-querier-timer** command configures the IGMP snooping querier other-querier-timer.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier other-querier-timer** <*other-querier-timer*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
other-querier-timer <*other-querier-timer*>	Specifies the IGMP snooping querier other-querier-timer. The value is an integer, in seconds, that ranges from 1 to 1000. The default value is 120.

Usage Guidelines

You can enable IGMP snooping querier function on the Layer 2 device to send IGMP query messages to take the querier role similar to Layer 3 multicast devices. If the Layer 2 querier receives an IGMP general query message sent by the upstream Layer 3 querier device, it will forward the IGMP general query message to all ports excluding the port receiving the messages of the VLAN. The IGMP snooping general query packets originally produced and planned to be sent by the Layer 2 querier devices are delayed and will be sent after the time of other-querier-timer.

Example

- Configure the IGMP snooping querier other-querier-timer.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier other-querier-timer 12
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier version

The **set protocols igmp-snooping vlan-id querier version** command configures the IGMP message version that the querier can support.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier version** <*querier-version*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
querier version <*querier-version*>	Specifies the IGMP message version that the querier supports. The value is **1** or **2**. • **1**: indicates that the querier processes only IGMPv1 messages. • **2**: indicates that the querier processes IGMPv1 and IGMPv2 messages. The default value is **2**.

Example

- Configure the IGMP snooping querier version.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier version 1
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id static group interface

The **set protocols igmp-snooping vlan-id static group interface** command configures a static member port to the particular multicast group.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **static group** <*group-address*> **interface** <*interface-name*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
group <*group-address*>	Specifies the IP address of a multicast group. The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
interface <*interface-name*>	Specifies the interface of the switch as a static member interface.

Usage Guidelines

In addition to dynamically establishing a multicast forwarding table through Layer 2 multicast protocols, you can manually configure the Layer 2 multicast forwarding entries to statically bind interfaces to multicast groups. After an interface is statically added to a multicast group, users on the interface can receive multicast data in the multicast group permanently and stably. Static member port will not be affected by the aging time, it will not age.

Example

- Configure a static member interface to the multicast group.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 static group 224.0.0.1 interface ge-1/1/3
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id unregistered flood-all

The **set protocols igmp-snooping vlan-id unregistered flood-all** command can be used to enable or disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **unregistered flood-all** <**true | false**>

Parameters

Parameter	Description
vlan-id <*vlan-id*>	Specifies the VLAN tag identifier. The valid VLAN ID range is 1-4094.
enable <**true	false**>	Enable or disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. • **true**: Enable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. • **false**: Disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. This function is disabled by default. Unknown multicast traffic can be forwarded to the router ports.

Example

- Enable unknown multicast traffic flooding in VLAN 100 with IGMP snooping enabled.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 100 unregistered flood-all true
admin@Xorplus# commit
```

IGMP Commands

- set protocols igmp interface
- set protocols igmp interface join-group
- set protocols igmp interface query-interval
- set protocols igmp interface query-max-response-time
- set protocols igmp interface version
- run show igmp groups
- run show igmp interface

set protocols igmp interface

The **set protocols igmp interface** command enables IGMP on an L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*>
delete protocols igmp interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.

Usage Guidelines

On a shared network segment, user hosts and Layer 3 multicast devices directly connected to the user network segment must run IGMP. A multicast device can process IGMP messages sent from user hosts only after IGMP is enabled on the interfaces connected to user network segments.

Example
• This example enables IGMP on vlan2:

```
admin@XorPlus# set protocols igmp interface vlan2
admin@XorPlus# commit
```

set protocols igmp interface join-group

The **set protocols igmp interface join-group** command configures a static multicast group on an L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*> **join-group** <*group-address*> [**source** <*source-address*>]

delete protocols igmp interface <*interface-name*> **join-group** <*group-address*> [**source** <*source-address*>]

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
join-group <*group-address*>	Specifies a multicast group address. In batch configuration mode, this parameter specifies the start address of the multicast group range. The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source <*source-address*>	Optional. Specifies a multicast source address. If the specified static group address is an SSM group address, you must specify a multicast source address for the group. The address is in dotted decimal notation.

Usage Guidelines

You can configure static multicast groups on user-side interfaces of the switch in some scenarios, for example:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

Note that: The IGMP entries of static groups configured on an interface never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment of the interface.

Example
• Configure static multicast group 224.1.1.1 on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 join-group 224.1.1.1
admin@XorPlus# commit
```

set protocols igmp interface query-interval

The **set protocols igmp interface query-interval** command sets the interval at which an L3 interface sends IGMP General Query messages.

Command Syntax
set protocols igmp interface <*interface-name*> **query-interval** <*query-interval*>

delete protocols igmp interface <*interface-name*> **query-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
query-interval <*query-interval*>	Specifies the interval at which an interface sends IGMP General Query messages. The value is an integer that ranges from 1 to 1800, in seconds.

Usage Guidelines

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network.

Example
• Configure the interval at which an interface sends IGMP General Query messages to 50 seconds on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 query-interval 50
admin@XorPlus# commit
```

set protocols igmp interface query-max-response-time

The **set protocols igmp interface query-max-response-time** command sets the maximum response time for IGMP General Query messages on an interface.

Command Syntax
set protocols igmp interface <*interface-name*> **query-max-response-time** <*interval*>

delete protocols igmp interface <*interface-name*> **query-max-response-time**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
query-max-response-time <*interval*>	Specifies the maximum response time for IGMP General Query messages. The value is an integer that ranges from 10 to 250, in deciseconds.

Usage Guidelines

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. The network may be congested when this situation occurs.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Example
• Set the maximum response time for IGMP General Query messages to 80 deciseconds on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 query-max-response-time 80
admin@XorPlus# commit
```

set protocols igmp interface version

Users can configure IGMP protocol version for a specified L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*> **version** <*number*>
delete protocols igmp interface <*interface-name*> **version**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
version <*number*>	The IGMP protocol version. The value could be **2** or **3**.

Usage Guidelines

The switch can identify IGMP messages of a version earlier than its own IGMP version but cannot identify IGMP messages of a later version. To ensure normal IGMP operation, ensure that the switch runs the same IGMP version as member hosts or a later IGMP version.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Example
• This example sets IGMP protocol version to 2 on vlan2:

```
admin@XorPlus# set protocols igmp interface vlan2 version 2
admin@XorPlus# commit
```

run show igmp groups

The **run show igmp groups** command displays information about all IGMP groups that hosts have joined by sending IGMP Report messages.

Command Syntax
run show igmp groups

Parameter

None.

Example
• Display information about all IGMP groups.

```
admin@XorPlus# run show igmp groups
Total IGMP groups: 6
Watermark warn limit(Not Set): 0
Interface   Group           Mode Timer    Srcs V Uptime
vlan2       224.0.0.2       INCL --:--:--    1 2 01:12:11
vlan2       224.0.0.22      INCL --:--:--    1 2 01:12:11
vlan2       238.255.0.1     INCL --:--:--    1 2 01:12:11
vlan3       224.0.0.2       INCL --:--:--    1 3 01:33:28
vlan3       224.0.0.22      INCL --:--:--    1 3 01:33:28
vlan3       238.255.0.2     INCL --:--:--    1 3 01:33:28
```

run show igmp interface

The **run show igmp interface** command displays information about IGMP interfaces.

Command Syntax
run show igmp interface [<*interface-name*>]

Parameter

Parameter	Description
<*interface-name*>	Optional. Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.

Example

- Display the IGMP configuration and running information on VLAN771.

```
admin@XorPlus# run show igmp interface vlan771
Interface : vlan2
State : up
Address : 5.5.5.5
Uptime : 00:00:10
Version : 3


Querier
-------
Querier : local
QuerierIp : 5.5.5.5 (this router)
Start Count : 0
Query Timer : 00:00:35
Other Timer : --:--:--


Timers
------
Group Membership Interval : 370s
Last Member Query Count : 2
Last Member Query Time : 2s
Older Host Present Interval : 370s
Other Querier Present Interval : 365s
Query Interval : 180s
Query Response Interval : 10s
Robustness Variable : 2
Startup Query Interval : 45s


Flags
-----
All Multicast : no
Broadcast : yes
Deleted : no
Interface Index : 94
Multicast : yes
Promiscuous : no
```

- Display information about all IGMP interfaces.

```
admin@XorPlus# run show igmp interface
Interface         State          Address  V  Querier  Query Timer    Uptime
vlan2              up        10.10.60.10  2    local     00:00:40  02:13:12
vlan3              up        10.10.61.10  3    local     --:--:--  00:36:29
```

PIM Configuration Commands

- set protocols pim ecmp
- set protocols pim interface active-active
- set protocols pim interface drpriority
- set protocols pim interface hello holdtime
- set protocols pim interface hello interval
- set protocols pim interface sm
- set protocols pim interface use-source
- set protocols pim join-prune-interval
- set protocols pim keep-alive-timer
- set protocols pim packets
- set protocols pim register-suppress-time
- set protocols pim rp
- set protocols pim spt-switchover infinity-and-beyond
- set protocols pim ssm prefix-list
- set protocols pim interface bsm
- set protocols pim interface unicast-bsm
- run show pim interface
- run show pim rp-info
- run show pim neighbor
- run show pim upstream
- run show mroute
- mtrace
- run show pim group-type
- run show pim bsr
- run show pim bsm-database
- run show pim bsrp-info
- run clear pim bsr-data

set protocols pim ecmp

The **set protocols pim ecmp** command is used to enable ECMP function for PIM.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] ecmp [rebalance]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

- If pim has the a choice of ECMP nexthops for a particular RPF, pim will cause S,G flows to be spread out amongst the nexthops. If this command is not specified then the first nexthop found will be used. This command is vrf aware, to configure for a vrf, specify the vrf name.
- If pim is using ECMP and an interface goes down, cause pim to rebalance all S,G flows across the remaining nexthops. If this command is not configured pim only modifies those S,G flows that were using the interface that went down.

Example

- Enable ECMP function for PIM.

```
admin@Xorplus# set protocols pim ecmp
admin@Xorplus# commit
```

set protocols pim interface active-active

The **set protocols pim interface active-active** command is used to turn on PIM active-active configuration. This command will not do anything if you do not have the underlying ability of a MLAG implementation.

The **delete protocols pim interface active-active** command is used to disable PIM active-active configuration.

Command Syntax

set protocols pim interface <*interface-name*> **active-active**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.

Usage Guidelines

For a multicast sender or receiver to be supported over a dual-attached MLAG bond, you must configure pim active-active.

Example

- Set the PIM active-active configuration.

```
admin@Xorplus# set protocols pim interface vlan-2 active-active
admin@Xorplus# commit
```

set protocols pim interface drpriority

The **set protocols pim interface drpriority** command is used to configure the Designated Router priority per interface.

Command Syntax

set protocols pim interface <*interface-name*> **drpriority** <*dr-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
drpriority <*dr-priority*>	Specifies the Designated Router priority. The greater the value, the higher the priority. The value is an integer that ranges from 1 to 4294967295. The default value is 1.

Usage Guidelines

The DR election is based on the priority and the IP address. To elect the DR, the PIM neighbors send the Hello message that contains the DR priority to each other. The switch with the highest priority functions as the DR. If the switches have the same priority, the switch with the largest IP address functions as the DR.

Example

- Configure the Designated Router priority for the PIM interface vlan-2 to 100.

```
admin@Xorplus# set protocols pim interface vlan-2 drpriority 100
admin@Xorplus# commit
```

set protocols pim interface hello holdtime

The **set protocols pim interface hello holdtime** command is used to configure the randomized triggered delay of PIM Hello messages (in seconds) per interface.

Command Syntax

set protocols pims interface <*interface-name*> **hello holdtime** < *interval*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
hello holdtime < *interval*>	Specifies the maximum delay for triggering Hello messages. The value is an integer that ranges from 3 to 65535 in seconds.

Usage Guidelines

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and hello-triggered-delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages must be sent every hello-period seconds.

Example

- Set the randomized triggered delay of PIM Hello messages to 10 seconds on vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 hello holdtime 10
admin@Xorplus# commit
```

set protocols pim interface hello interval

The **set protocols pim interface hello interval** command configures the PIM Hello messages period (in seconds) per interface.

Command Syntax

set protocols pim interface <*interface-name*> **hello interval** <*interval*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
hello interval <*interval*>	Specifies the interval for sending Hello messages. The value is an integer that ranges from 1 to 65535, in seconds.

Usage Guidelines

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the this command to set the interval for sending Hello messages. The neighbor holdtime is 3.5 * hello-period.

Example

- Set the interval for sending Hello messages to 40 seconds on vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 hello interval 40
admin@Xorplus# commit
```

set protocols pim interface sm

The **set protocols pim interface sm** command is used to enable PIM-SM function on a specific L3 interface.

The **delete protocols pim interface sm** command is used to disable PIM-SM function on a specific L3 interface.

Command Syntax

set protocols pim interface <*interface-name*> **sm**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.

Example

- Enable PIM-SM function on the L3 VLAN interface vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 sm
admin@Xorplus# commit
```

set protocols pim interface use-source

The **set protocols pim interface use-source** command is used to configure the source IP address.

Command Syntax

set protocols pim interface <*interface-name*> **use-source** <*source-ip*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
use-source <*source-ip*>	Specifies the source IP address.

Usage Guidelines

If you have multiple addresses configured on a particular interface and would like pim to use a specific source address associated with that interface.

Example

- Configure the source IP address for the PIM interface vlan-2 to 192.168.10.1.

```
admin@Xorplus# set protocols pim interface vlan-2 use-source 192.168.10.1
admin@Xorplus# commit
```

set protocols pim join-prune-interval

The **set protocols pim join-prune-interval** command configures the frequency at which the router will send periodic join or prune-interval messages.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] join-prune-interval** <*interval-value*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
join-prune-interval <*interval-value*>	Specifies the join-prune-interval in seconds. Range 1 to 65535.

Usage Guidelines

If pim has the a choice of ECMP nexthops for a particular RPF, pim will cause S,G flows to be spread out amongst the nexthops. If this command is not specified then the first nexthop found will be used. This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure join prune interval:

```
admin@Xorplus# set protocols pim join-prune-interval 120
admin@Xorplus# commit
```

set protocols pim keep-alive-timer

The **set protocols pim keep-alive-timer** command modifies the time out value for a S,G flow from 1-65535 seconds.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] keep-alive-timer** <*interval*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
keep-alive-timer <*interval*>	Specifies the time out value for a S,G flow in seconds. Range 1 to 65535.

Usage Guidelines

This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure the time out value for a S,G flow.

```
admin@Xorplus# set protocols pim keep-alive-timer 120
admin@Xorplus# commit
```

set protocols pim packets

The **set protocols pim packets** command configures the max number of packets incoming that can be processed at one time when processing packets from a neighbor.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] packets** <*packets-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
packets <*packets-number*>	Specifies the max number of packets incoming that can be processed at one time. The value is an integer that ranges from 1 to 255.

Usage Guidelines

When processing packets from a neighbor process the number of packets incoming at one time before moving on to the next task. The default value is 3 packets. This command is only useful at scale when you can possibly have a large number of pim control packets flowing. This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure the max number of packets incoming that can be processed at one time.

```
admin@Xorplus# set protocols pim packets 50
admin@Xorplus# commit
```

set protocols pim register-suppress-time

The **set protocols pim register-suppress-time** command modifies the time that PIM will register suppress a FHR will send register notifications to the kernel.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] register-suppress-time** <*interval*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
register-suppress-time <*interval*>	Specifies the register suppress time. The value is an integer in seconds that ranges from 1 to 65535.

Example

- Configure the register suppress time.

```
admin@Xorplus# set protocols pim register-suppress-time 50
admin@Xorplus# commit
```

set protocols pim rp

The **set protocols pim rp** command statically configures a static RP for a specified multicast group.

Command Syntax

set protocols pim [vrf<*vrf-name*>] rp <*rp-address*> [**group** <*group-address*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
rp <*rp-address*>	Specifies the address of the static RP in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
group <*group-address*>	Optional. Specifies the multicast group address in IPv4/prefix-lenghth format.

Usage Guidelines

This command must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv4 multicast addresses (224.0.0.0 - 239.255.255.255).

Example

- Configure the router as the RP.

```
admin@Xorplus# set protocols pim rp 10.110.0.6
admin@Xorplus# commit
```

set protocols pim spt-switchover infinity-and-beyond

The **set protocols pim spt-switchover** command configures SPT switchover on a per-group basis, allowing for some groups to never switch to a shortest path tree.

Command Syntax

set protocols pim [vrf<*vrf-name*>] spt-switchover infinity-and-beyond prefix-list <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
prefix-list <*prefix-list*>	Specifies the prefix-list name. The value is a string which has been set by comannd set routing prefix-list.

Usage Guidelines

When the LHR receives the first multicast packet, it sends a PIM (S,G) join towards the FHR to efficiently forward traffic through the network. This builds the shortest path tree (SPT), or the tree that is the shortest path to the source. When the traffic arrives over the SPT, a PIM (S,G) RPT prune is sent up the shared tree towards the RP. This removes multicast traffic from the shared tree; multicast data is only sent over the SPT.

You can configure SPT switchover on a per-group basis, allowing for some groups to never switch to a shortest path tree; this is also called SPT infinity. The LHR now sends both (*,G) joins and (S,G) RPT prune messages towards the RP.

To configure a group to never follow the SPT, create the necessary prefix lists, then configure SPT switchover for the prefix-list.

Example

- The following example is to configure a group to never follow the SPT, create the necessary prefixlists, then configure SPT switchover for the spt-range prefix-list:

```
admin@Xorplus# set routing prefix-list IPv4 spt-range seq 1 permit prefix 235.0.0.0/8 ge 32
admin@Xorplus# set routing prefix-list IPv4 spt-range seq 1 permit prefix 238.0.0.0/8 ge 32
admin@Xorplus# set protocols pim spt-switchover infinity-and-beyond prefix-list spt-range
admin@Xorplus# commit
```

set protocols pim ssm prefix-list

The **set protocols pim ssm prefix-list** command sets a range of group addresses via a prefix-list that forces pim to never do SM over.

Command Syntax

set protocols pim [vrf<*vrf-name*>] ssm prefix-list <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
prefix-list <*prefix-list*>	Specifies the prefix-list name. The value is a string which has been set by comannd set routing prefix-list.

Example

- Configure a range of group addresses via a prefix-list.

```
admin@Xorplus# set protocols pim ssm prefix-list PreLst1
admin@Xorplus# set routing prefix-list ipv4-family PreLst1 permit prefix 233.0.0.0/8
admin@Xorplus# set routing prefix-list ipv4-family PreLst1 permit prefix 232.0.0.0/8
admin@Xorplus# commit
```

set protocols pim interface bsm

The **set protocols pim interface bsm** command is used to configure the handling of bootstrap messages (BSM) on a specific VLAN interface for Protocol Independent Multicast (PIM).

The **delete protocols pim interface bsm** command restores the default configuration.

Command Syntax

set protocols pim interface <*interface-name*> **bsm** <**enable** | **disable**>

delete protocols pim interface <*interface-name*> **bsm**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name. The value is a string.
<**enable** | **disable**>	Enables or disables the PIM interface to process bootstrap messages. The value is **enable** or **disable**. • **enable**: enables the PIM interface to process bootstrap messages. • **disable**: disables the PIM interface to process bootstrap messages. The default value is **enable**.

Usage Guidelines

By enabling or disabling the processing of bootstrap messages on a PIM interface, network administrators can control how the interface participates in the PIM-SM (Sparse Mode) Bootstrap Router mechanism. Enabling BSM handling allows the interface to participate in the dynamic election of RPs and BSRs, improving multicast routing efficiency and resilience.

> **NOTE:**
>
> When the PIM-SM Bootstrap Router mechanism is enabled to dynamically elect an RP, the PICOS switch can receive C-RP advertisement messages sent by other PIM switches. It can then calculate and compare these messages to elect the RP for a specific group from multiple C-RPs. However, the PICOS switch itself does not participate in the election as a BSR or dynamic RP.

Example

- Enable the PIM interface to process bootstrap messages.

```
admin@PICOS# set protocols pim interface vlan2 bsm enable
admin@PICOS# commit
```

set protocols pim interface unicast-bsm

The **set protocols pim interface unicast-bsm** command is used to configure the handling of unicast bootstrap messages (BSM) on a specific VLAN interface for Protocol Independent Multicast (PIM).

The **delete protocols pim interface unicast-bsm** command is used to restore the default configuration.

Command Syntax

set protocols pim interface <*interface-name*> **unicast-bsm** <**enable** | **disable**>

delete protocols pim interface <*interface-name*> **unicast-bsm**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name. The value is a string.
<**enable** | **disable**>	Enables or disables the PIM interface to process unicast bootstrap messages. The value is **enable** or **disable**. • **enable**: enables the PIM interface to process unicast bootstrap messages. • **disable**: disables the PIM interface to process unicast bootstrap messages. The default value is **enable**.

Usage Guidelines

By enabling or disabling the processing of unicast bootstrap messages on a PIM interface, network administrators can control how the interface participates in the PIM-SM (Sparse Mode) Bootstrap Router mechanism. Enabling unicast BSM handling allows the interface to participate in the dynamic election of RPs and BSRs using unicast messages, improving multicast routing efficiency and resilience. Disabling it can be useful for optimizing network performance and ensuring the correct handling of multicast traffic based on specific network design requirements.

Example

- Enable the PIM interface to process unicast bootstrap messages.

```
admin@PICOS# set protocols pim interface vlan2 unicast-bsm enable
admin@PICOS# commit
```

run show pim interface

The **run show pim interface** command shows information about all interfaces on which PIM-SM is enabled.

Command Syntax

run show pim interface [**detail**]

Parameter

None.

Example

- Show information about all interfaces on which PIM-SM is enabled.

```
admin@Xorplus# run show pim interface
Interface      State        Address    PIM Nbrs     PIM DR       FHR      IfChannels
----------   --------   ------   --------   --------   ----   ---------
loopback    up      1.1.1.1    0           local        0        0
vlan100        up           10.0.0.11  1            10.0.0.21    0        4
```

run show pim rp-info

The **run show pim rp-info** command displays RP information for all the multicast groups.

Command Syntax
run show pim rp-info

Parameter

None.

Example

• Display RP information for all the multicast groups.

```
admin@PICOS# run show pim rp-info
RP address       group/prefix-list   OIF              I am RP    Source
3.3.3.3          224.1.1.1/32        vlan4094         no        Static
3.3.3.3          230.1.1.1/32        vlan4094         no        Static
3.3.3.3          231.1.1.1/32        vlan4094         no        Static
```

run show pim neighbor

The **run show pim neighbor** command shows information about PIM neighbors.

Command Syntax

run show pim neighbor

Parameter

None.

Example

- Show information about PIM neighbors.

```
admin@Xorplus# run show pim neighbor
Interface    Neighbor    Uptime       Holdtime     DR Pri
----------  ----------  ----------  ----------  ----------
vlan20       20.0.0.2     105          84           1
```

run show pim upstream

The **run show pim upstream** command displays upstream information about a S,G mroute.

Command Syntax

run show pim upstream

Parameter

None.

Example

- Show the upstream information about a S,G mroute.

```
admin@Xorplus# run show pim upstream
Iif Source       Group     State Uptime   JoinTimer RSTimer KATimer  RefCnt
br0 172.16.5.105 239.1.1.1 Prune 00:07:40 --:--:-- 00:00:36 00:02:50 1
!
```

run show mroute

The **run show mroute** command displays the PIM routing table information.

Command Syntax
run show mroute [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

- Display the PIM routing table.

```
admin@XorPlus# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group           Flags   Proto  Input            Output           TTL  Uptime
71.1.1.100      231.1.1.1       SFP             none   vlan771          none             0    --:--:--
81.1.1.100      231.1.1.1       SCT             IGMP   vlan4000         vlan771          1    00:03:57
```

mtrace

The **mtrace** command displays multicast traceroute towards specified IPv4 source and group address.

Command Syntax

- From the ">" prompt, use the following format,

mtrace source <*ipv4-src-addr*> [**group** <*ipv4-group-addr*>]

- From the "#" prompt, add **run** in front of the command,

run mtrace source <*ipv4-src-addr*> [**group** <*ipv4-group-addr*>]

Parameters

Parameter	Description
source <*ipv4-src-addr*>	Specifies the source IPv4 address to trace.
group <*ipv4-group-addr*>	Optional. Specifies the group IPv4 address to trace.

Example

- The following example traces with multicast source:

```
admin@PICOS> mtrace source 1.1.1.100
* Mtrace from 1.1.1.100 to 3.3.3.30 via group 0.0.0.0
Querying full reverse path...
 * switching to hop-by-hop:
  0  ? (3.3.3.30)
 -1  ? (3.3.3.3) PIM thresh^ 1
Round trip time 3 ms; total ttl of 1 required.
```

- The following example traces with multicast source and group address:

```
admin@PICOS# run mtrace source 1.1.1.100 group 224.1.1.1
* Mtrace from 1.1.1.100 to 3.3.3.30 via group 224.1.1.1
Querying full reverse path...
 * switching to hop-by-hop:
  0  ? (3.3.3.30)
 -1  ? (3.3.3.3) PIM (S,G) thresh^ 1
Round trip time 3 ms; total ttl of 1 required.
```

In the display result, "0" represents the switch currently executing mtrace, "-1" represents the first hop starting from the current switch and its interface IP address is 3.3.3.3.

run show pim group-type

The **run show pim group-type** command display SSM group ranges.

Command Syntax

run show pim group-type

Parameters

None.

Example

- This example shows how to display information about PIM group ranges:

```
admin@Xorplus# run show pim group-type
SSM group range : 232.0.0.0/8
```

run show pim bsr

The **run show pim bsr** command displays current BSR, its uptime and last received BSM age.

Command Syntax

run show pim bsr

Parameter

None.

Example

- Display current BSR, its uptime and last received BSM age.

```
admin@PICOS# run show pim bsr
PIMv2 Bootstrap information
Current preferred BSR address: 10.10.10.11
Priority        Fragment-Tag       State                UpTime
  0               2400           ACCEPT_PREFERRED       00:20:00
Last BSM seen: 00:00:10
```

run show pim bsm-database

The **run show pim bsm-database** command display all fragments of stored bootstrap message in user readable format.

Command Syntax

run show pim bsm-database

Parameter

None.

Example

- Display all fragments of stored bootstrap message in user readable format.

```
admin@PICOS# run show pim bsm-database
Scope Zone: Global
Number of the fragments: 0
```

run show pim bsrp-info

The **run show pim bsrp-info** command displays group-to-rp mappings received from E-BSR.

Command Syntax

run show pim bsrp-info

Parameter

None.

Example

- Display group-to-rp mappings received from E-BSR.

```
admin@PICOS# run show pim bsrp-info
BSRP address: 0.0.0.0
```

run clear pim bsr-data

The **run clear pim bsr-data** command clears the BSM scope data struct. This command also removes the next hop tracking for the bsr and resets the upstreams for the dynamically learnt RPs.

Command Syntax

run clear pim [**vrf** <*text*>] **bsr-data**

Parameter

Parameter	Description
vrf <*text*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

- Clear the BSM scope data struct.

```
admin@PICOS# run clear pim bsr-data
```

Multicast Source Discovery Protocol (MSDP) Commands

- set protocols msdp mesh-group source
- set protocols msdp mesh-group member
- run show msdp mesh-group
- run show msdp peer
- run show msdp sa

set protocols msdp mesh-group source

The **set protocols msdp mesh-group source** command is used to configure the source address of MSDP peers.

Command Syntax

set protocols msdp mesh-group < *mesh-group-name*> **source** <*source-address*>

Parameter

Parameter	Description
mesh-group < *mesh-group-name*>	Specifies the name of the MSDP mesh group. The value is a string.
source <*source-address*>	Specifies the address of the local RP device as the source address of the local MSDP device. The value is in dotted decimal format.

Usage Guidelines

Only one mesh group is allowed in one PIM-SM domain.

When configuring MSDP peers, configure the local MSDP device as the source and all the other remote MSDP peer devices in the same mesh group as members.

Example

- Create an MSDP mesh group.

```
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Xorplus# commit
```

set protocols msdp mesh-group member

The **set protocols msdp mesh-group member** command is used to configure the MSDP member devices.

Command Syntax

set protocols msdp mesh-group < *mesh-group-name*> **member** <*peer-address*>

Parameter

Parameter	Description
mesh-group < *mesh-group-name*>	Specifies the name of the MSDP mesh group. The value is a string.
member <*peer-address*>	Specifies the address of the remote MSDP peer that becomes a MSDP member. The value is in dotted decimal format.

Usage Guidelines

Only one mesh group is allowed in a PIM-SM domain.

When configuring MSDP peers, configure the local MSDP device as the source and all the other remote MSDP peer devices in the same mesh group as members.

Example

- Create an MSDP mesh group.

```
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Xorplus# commit
```

run show msdp mesh-group

The **run show msdp mesh-group** command displays the establishment state of MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp mesh-group

Parameter

Null.

Example

- View the establishment state of MSDP peers.

```
admin@Xorplus# run show msdp mesh-group
Mesh group : 6.6.6.6
  Source : 2.2.2.2
  Member         State
  3.3.3.3          established
```

run show msdp peer

The **run show msdp peer** command displays the status information of the MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp peer [*<peer-ip>* | **detail**]

Parameter

Parameter	Description
<peer-ip>	Optional. Specifies the address of a remote MSDP peer. If this parameter is not specified, information about all the MSDP peers will be displayed. The address is in dotted decimal notation.
detail	Optional. Displays detail information about the status of MSDP peers.

Example

- View the brief information about all the remote MSDP peers.

```
admin@Xorplus# run show msdp peer
Peer                      Local        State    Uptime   SaCnt
3.3.3.3                 2.2.2.2  established  06:10:45       2
```

- View the detail information about all the remote MSDP peers.

```
admin@Xorplus# run show msdp peer detail
Peer : 3.3.3.3
  Local               : 2.2.2.2
  Mesh Group          : 6.6.6.6
  State               : established
  Uptime              : 06:10:52
  Keepalive Timer     : 00:00:08
  Conn Retry Timer    : --:--:--
  Hold Timer          : 00:00:46
  Last Reset          : -
  Conn Attempts       : 22
  Established Changes : 1
  SA Count            : 2
  Statistics          :
                       Sent       Rcvd
    Keepalives :        371          4
    SAs        :          0        748
```

- View the detail information about a specific remote MSDP peer.

```
admin@Xorplus# run show msdp peer 3.3.3.3
Peer : 3.3.3.3
  Local               : 2.2.2.2
  Mesh Group          : 6.6.6.6
  State               : established
  Uptime              : 06:11:03
  Keepalive Timer     : 00:00:57
  Conn Retry Timer    : --:--:--
  Hold Timer          : 00:00:35
  Last Reset          : -
  Conn Attempts       : 22
  Established Changes : 1
  SA Count            : 2
  Statistics          :
                       Sent       Rcvd
    Keepalives :        372          4
```

```
    SAs         :           0         748
```

run show msdp sa

The **run show msdp sa** command displays the (S, G) entries cached on MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp sa [**ip** <*ip-address*> | **detail**]

Parameter

Parameter	Description
ip <*ip-address*>	Optional. Specifies the address of a multicast source. If this parameter is not specified, (S, G) entries from all the multicast sources will be displayed. The address is in dotted decimal notation.
detail	Optional. Displays detail information about (S, G) entries cached on the device.

Example

- View the brief information about all (S, G) entries cached on the device.

```
admin@Xorplus# run show msdp sa
Source               Group            RP      Local  SPT  Uptime
200.200.200.2         237.0.0.2          3.3.3.3      n    y  00:15:17
200.200.200.2         237.0.0.3          3.3.3.3      n    y  00:13:35
```

- View the detail information about all (S, G) entries cached on the device.

```
admin@Xorplus# run show msdp sa detail
SA : (200.200.200.2,237.0.0.1)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 05:27:01
  State Timer : 00:02:34

SA : (200.200.200.2,239.255.255.250)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 06:04:55
  State Timer : 00:02:34
```

- View the detail (S, G) entries information of a specific multicast source cached on the device.

```
admin@Xorplus# run show msdp sa ip 200.200.200.2
SA : (200.200.200.2,237.0.0.1)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 05:27:33
  State Timer : 00:03:02

SA : (200.200.200.2,239.255.255.250)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 06:05:27
```

```
State Timer : 00:03:02
```

Multicast VLAN Registration (MVR) Commands

- run show igmp-snooping mvr mvlan
- run show igmp-snooping mvr receiver-vlan
- set protocols igmp-snooping vlan-id mvr receiver vlan-list
- set protocols igmp-snooping vlan-id mvr source group

run show igmp-snooping mvr mvlan

The **run show igmp-snooping mvr mvlan** command is used to view MVLAN information.

Command Syntax

run show igmp-snooping mvr mvlan <*vlan id*>

Parameter

Parameter	Description
<*vlan-id*>	The VLAN ID of the given MVLAN

Example

- View MVR interface information.

```
admin@PICOS# run show ipmp-snooping mvr mvlan 100
Mvlan     Receiver-vlan
--------  ---------------
100        101, 102, 103
```

run show igmp-snooping mvr receiver-vlan

The **run show igmp-snooping mvr receiver-vlan** command shows information of the given receiver VLAN ID.

Command Syntax

run show igmp-snooping mvr receiver-vlan <*vlan-id*>

Parameter

Parameter	Description
<*vlan-id*>	The VLAN ID of the given receiver VLAN.

Example

- View the brief information of the MVRP receiver VLAN.

```
admin@PICOS# run show igmp-snooping mvr receiver-vlan 101
Receiver-vlan   Mvlan
-------------  --------------
101             100
```

set protocols igmp-snooping vlan-id mvr receiver vlan-list

The **set protocols igmp-snooping vlan-id mvr receiver vlan-list** command configure the MVR mapped VLAN IDs on the access ports.

The **delete protocols igmp-snooping vlan-id mvr receiver vlan-list** command deletes the configuration.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mvr receiver vlan-list** <*vlan-range-string*>

delete protocols igmp-snooping vlan-id <*vlan-id*> **mvr receiver vlan-list**

Parameters

Parameter	Description
<*vlan-id*>	The multicast MVR VLAN ID.
<*vlan-range-string*>	The mapped receiver VLAN list for the given MVLAN.

Usage Guidelines

The IGMP query packets and stream traffic from the upstream port is updated to different VLAN ID in the vlan-list of the above configuration command. On the reverse direction, the IGMP report packets with the VLAN ID in the vlan-list are translated to the MVLAN accordingly.

The upstream traffic will go the trunk ports which have the VLAN ID as MVLAN.

Example

- Configure the receiver VLAN range as 101-199 for MVLAN 100.

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 mvr receiver vlan-list 101-199
admin@PICOS# commit
```

set protocols igmp-snooping vlan-id mvr source group

The **set protocols igmp-snooping vlan-id mvr source group** command can be used to configure the source multicast group of a given MVLAN.

The **delete protocols igmp-snooping vlan-id mvr source group** command deletes the configuration.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mvr source group** <*multicast-network-address*>/<*prefix-length*>

delete protocols igmp-snooping vlan-id <*vlan-id*> **mvr source group** <*multicast-network-address*>/<*prefix-length*>

Parameters

Parameter	Description
<*vlan-id*>	The MVLAN ID of the MVR multicast traffic from upstream.
<*multicast-network-address*>	The multicast group address of the MVR mapping.
<*prefix-length*>	The prefix length of the group address.

Usage Guidelines

Multiple source groups could be configured with one MVR VLAN instance.

Group overlapping is not allowed when configuring multiple MVLANs.

Example

- Configure the multicast source group range 225.0.0.1/8 for the given MVLAN 100.

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 mvr source group 225.0.0.1/8
admin@PICOS# commit
```

OpenFlow Commands in CrossFlow Mode

To use the hybrid mode of the Openflow switch, enable the xovs mode in XorPlus system. Next, configure the interfaces to be used in XorPlus system. Then, exit to Linux system to add the flows required.

Commands

set xovs enable ***<true | false>***

set interface gigabit-ethernet ge-1/1/1 crossflow enable true

set interface gigabit-ethernet ge-1/1/1 crossflow local-control false

set vlans vlan-id ***<vlan-id>***

delete xovs

set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk

set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members ***<vlan-id>***

VXLAN Commands

- set vxlans source-interface address
- OVSDB VTEP command
  - set protocols ovsdb controller vrf mgmt-vrf
  - set protocols ovsdb controller address
  - set protocols ovsdb controller inactivity-probe-duration
  - set protocols ovsdb controller maximum-backoff-duration
  - set protocols ovsdb controller port
  - set protocols ovsdb controller protocol
  - set protocols ovsdb interface
  - set protocols ovsdb management-ip
  - set protocols ovsdb ssl bootstrap
  - set protocols ovsdb ssl ca-cert
  - set protocols ovsdb ssl certificate
  - set protocols ovsdb ssl private-key
- set vxlans l3-vni prefix-routes-only
- set vxlans vni mcast-group
- run show vxlan statistics
- run clear vxlan statistics
- set vxlans udp-port
- run show vxlan vni
- run show vxlan address-table
- run show vxlan arp
- run show vxlan l3-vni entry
- run show vxlan neighbor
- set vxlans vni decapsulation mode
- set vxlans vni encapsulation mode
- set vxlans vni encapsulation vlan
- set vxlans vni flood vtep
- set vxlans vni flood vtep mac-address
- set vxlans vni flood vtep traffic-type
- set vxlans vni vlan
- set vxlans tunnel-mac-leaning disable
- set vxlans l3-vni

set vxlans source-interface address

User can configure vxlan source interface ip address .

Command Syntax

set vxlans source-interface <*interface*> **address** <*ipv4-addr*>

delete vxlans source-interface <*interface*> **address**

Parameters

Parameter	Description
source-interface <*interface*>	The vlan interface, e.g. loopback or vlan10.
address <*ipv4-addr*>	The IPv4 address.

Example

• This example demonstrates how to configure the vxlan to use the IP address 10.10.10.1 as the source address in the encapsulation fields of outbound VXLAN frames.

```
XorPlus# set vxlans source-interface loopback address 10.10.10.1
XorPlus# commit
```

OVSDB VTEP command

- set protocols ovsdb controller vrf mgmt-vrf
- set protocols ovsdb controller address
- set protocols ovsdb controller inactivity-probe-duration
- set protocols ovsdb controller maximum-backoff-duration
- set protocols ovsdb controller port
- set protocols ovsdb controller protocol
- set protocols ovsdb interface
- set protocols ovsdb management-ip
- set protocols ovsdb ssl bootstrap
- set protocols ovsdb ssl ca-cert
- set protocols ovsdb ssl certificate
- set protocols ovsdb ssl private-key

set protocols ovsdb controller vrf mgmt-vrf

The **set protocols ovsdb controller vrf mgmt-vrf** command configures to run the Open vSwitch Database (OVSDB) management protocol in the management VRF.

Command Syntax

set protocols ovsdb controller *<controller-name>* **vrf mgmt-vrf**

Parameter

Parameter	Description
controller *<controller-name>*	Specifies the OVSDB controller name. The value is a string.

Usage Guidelines

OVSDB management protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding OVSDB controller is required to be route reachable in the VRF running OVSDB management protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the OVSDB management protocol to run in the management VRF.

```
admin@Xorplus# set protocols ovsdb controller c1 vrf mgmt-vrf
admin@Xorplus# commit
```

set protocols ovsdb controller address

User can configure ovsdb vtep to establish an active OVSDB tcp/ssl connection to a controller.

Command Syntax

set protocols ovsdb controller <*controller-name*> **address** <*ip-addr*>

delete protocols ovsdb controller <*controller-name*> **address**

Parameters

Parameter	Description
controller <*controller-name*>	controller name.
address <*ip-addr*>	Specifies the destination IPv4/IPv6 address for the tcp/ssl connection.

Example

• This example demonstrates how to configure a tcp/ssl connection to port 6632 at 10.10.50.220.

```
admin@XorPlus# set protocols ovsdb controller c1 address 10.10.50.220
admin@XorPlus# commit
```

set protocols ovsdb controller inactivity-probe-duration

User can configure ovsdb vtep tcp/ssl connection inactivity probe duration.

Command Syntax

set protocols ovsdb controller <*controller-name*> **inactivity-probe-duration** <*uint*>

delete protocols ovsdb controller <*controller-name*> **inactivity-probe-duration**

Parameters

Parameter	Description
controller <*controller-name*>	Controller name.
inactivity-probe-duration <*uint*>	Number of milliseconds the connection can be inactive before an inactivity probe is sent.

Example

• This example demonstrates how to configure a tcp/ssl connection inactivity probe duration.

```
admin@XorPlus# set protocols ovsdb controller c1 inactivity-probe-duration 30001
admin@XorPlus# commit
```

set protocols ovsdb controller maximum-backoff-duration

User can configure ovsdb vtep tcp/ssl connection maximum backoff duration.

Command Syntax

set protocols ovsdb controller <*controller-name*> **maximum-backoff-duration** <*uint*>

delete protocols ovsdb controller <*controller-name*> **maximum-backoff-duration**

Parameters

Parameter	Description
controller <*controller-name*>	Controller name.
maximum-backoff-duration <*uint*>	Number of milliseconds OVSDB server waits before it re-attempts to connect with an controller, the valid VLAN numbers range 1000-4294967295.

Example

• This example demonstrates how to configure a tcp/ssl connection maximum backoff duration.

```
admin@XorPlus# set protocols ovsdb controller c1 maximum-backoff-duration 1001
admin@XorPlus# commit
```

set protocols ovsdb controller port

User can configure ovsdb vtep tcp/ssl connection port number.

Command Syntax

set protocols ovsdb controller <*controller-name*> **port** <*port-number*>

delete protocols ovsdb controller <*controller-name*> **port**

Parameters

Parameter	Description
controller <*controller-name*>	Controller name.
port <*port-number*>	Specifies the destination port or listen port for the tcp/ssl connection. The value range for the port-number argument is 0 to 65535.

Example

This example demonstrates how to configure an tcp/ssl connection port.

```
admin@XorPlus# set protocols ovsdb controller c1 port 6632
admin@XorPlus# commit
```

set protocols ovsdb controller protocol

User can configure ovsdb vtep establish connection with protocol.

Command Syntax

set protocols ovsdb controller <*controller-name*> **protocol** <*protocol-mode*>

delete protocols ovsdb controller <*controller-name*> **protocol**

Parameters

Parameter	Description
controller <*controller-name*>	Controller name.
protocol <*protocol-mode*>	Configure establish an OVSDB SSL or TCP connection with a one controller or listen for OVSDB SSL or TCP connection requests: • **pssl** Listening for SSL connection requests from controllers • **ptcp** Listening for TCP connection requests from controllers • **ssl** Establishing an active SSL connection to a controller • **tcp** Establishing an active TCP connection to a controller

Example

This example demonstrates how to configure ovsdb vtep establish connection protocol with ptcp

```
admin@XorPlus# set protocols ovsdb controller c1 protocol ptcp
admin@XorPlus# commit
```

set protocols ovsdb interface

User can configure ovsdb vtep access port.

Command Syntax
set protocols ovsdb interface <*interface-name*>

delete protocols ovsdb interface <*interface-name*>

Parameters

Parameter	Description
interface <*interface-name*>	Specify the interface name as a OVSDB vtep access port.

Example
• This example demonstrates how to configure specify te-1/1/1 as a ovsdb vtep access port.

```
admin@XorPlus# set protocols ovsdb interface te-1/1/1
admin@XorPlus# commit
```

set protocols ovsdb management-ip

User can configure ovsdb vtep access port.

Command Syntax

set protocols ovsdb management-ip <*ipv4/ipv6*>

delete protocols ovsdb management-ip <*ipv4/ipv6*>

Parameters

Parameter	Description
management-ip <*ipv4/ipv6*>	IPv4 or IPv6 address, configuring the OVSDB VTEP's management IP for controller.

Example

• This example demonstrates how to configure the VTEP's management IP.

```
admin@XorPlus# set protocols ovsdb management-ip 10.10.51.157
admin@XorPlus# commit
```

set protocols ovsdb ssl bootstrap

User can configure obtain the CA certificate from the SSL peer.

Command Syntax
set protocols ovsdb SSL bootstrap <*boolean*>

delete protocols ovsdb ssl bootstrap

Parameters

Parameter	Description
<*boolean*>	Enable or disable ssl bootstrap. • **true** enable ssl bootstrap, the ca certificate automatically downloaded from ssl peer. • **false** disable ssl bootstrap, the ca certificate manually copy to the /ovs/var/lib/openvswitch/pki directory

Example
• This example demonstrates how to configure ovsdb ssl bootstrap.

```
admin@XorPlus# set protocols ovsdb SSL bootstrap true
admin@XorPlus# commit
```

set protocols ovsdb ssl ca-cert

User can configure CA certificate file for ssl connected.

Command Syntax
set protocols ovsdb ssl ca-cert <*file*>

delete protocols ovsdb ssl ca-cert

Parameters

Parameter	Description
ca-cert <*file*>	Specifies ssl connect with CA certificate file name.

Example
• This example demonstrates how to configure CA certificate file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl ca-cert "/ovs/var/lib/openvswitch/pki/controller.cacert"
admin@XorPlus# commit
```

set protocols ovsdb ssl certificate

User can configure certificate file for ssl connected.

Command Syntax
set protocols ovsdb ssl certificate <*file*>

delete protocols ovsdb ssl certificate

Parameters

Parameter	Description
certificate <*file*>	Specifies ssl connect with certificate file name.

Example
• This example configure certificate file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl certificate "/ovs/var/lib/openvswitch/pki/pica8-cert.pem"
admin@XorPlus# commit
```

set protocols ovsdb ssl private-key

User can configure a private key file for ssl connected.

Command Syntax

set protocols ovsdb ssl private-key <*file*>

delete protocols ovsdb ssl private-key

Parameters

Parameter	Description
private-key <*file*>	Specifies ssl connect with private key file name.

Example

• This example demonstrates how to configure private key file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl private-key "/ovs/var/lib/openvswitch/pki/pica8-privkey.pem"
admin@XorPlus# commit
```

set vxlans l3-vni prefix-routes-only

Run the command **set vxlans l3-vni prefix-routes-only** to advertise the prefix routes only. Without this command prefix routes wont be advertised to the peer devices.

Note that this configuration its mandatory in asymmetric EVPN routing model where we want to advertise the Type-5 prefix routes. In symmetric EVPN routing model however, we will use the command **set vxlans l3-vni** <vni-id> to advertise host routes as Type-2 advertisements and Type-5 prefix routes.

Command Syntax

set vxlans vrf <*vrf-name*> **l3-vni** <*vni-id*> **prefix-routes-only**

delete vxlans vrf <*vrf-name*> **l3-vni** <*vni-id*> **prefix-routes-only**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional, specifies the VRF name.
l3-vni <*vni-id*>	Specifies the layer 3 VNI ID.

Example

- This example demonstrates how to enable prefix routes only advertisement as Type-5 routes for a given VRF.

```
admin@XorPlus# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
admin@XorPlus# commit
```

set vxlans vni mcast-group

The **set vxlans vni mcast-group** command is used to enable the multicast replication function of BUM message and to configure the multicast replication address of VNI.

> **NOTE:**
> PICOS supports only one VXLAN segment mapping to one IP multicast group, which is the way to provide the optimal multicast forwarding. That is, to have multiple VXLAN segments share a single IP multicast group in the core network is not supported.

Command Syntax

set vxlans vni <*vni-id*> **mcast-group** <*ip-address*>

delete vxlans vni <*vni-id*> **mcast-group** <*ip-address*>

Parameters

Parameter	Description
vni <*vni-id*>	Specifies the layer 3 VNI ID.
mcast-group <*ip-address*>	Specifies the multicast replication address.

Example

- This example enables the multicast replication function.

```
admin@XorPlus# set vxlans vni 1 mcast-group  1.1.1.1
admin@XorPlus# commit
```

run show vxlan statistics

The **run show vxlan statistics** command shows traffic statistics of the VXLAN tunnel.

Command Syntax

run show vxlan statistics [**vni** <*vni-id*>]

Parameter

Parameter	Description
vni <*vni-id*>	Optional. Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200. If VNI ID is specified, it will only show the statistics of the specified VXLAN tunnel. If VNI ID is not specified, it will show the statistics of all the VXLAN tunnels.

Example

- Show traffic statistics of the VXLAN tunnel.

```
admin@Xorplus# run show vxlan statistics
VNID     Interface    Vlan ID  Type       Input(Pkts)           Output(Pkts)        Input(Octets)         Output(Oc
-------- ------------ ------- ----------- --------------------- ------------------- --------------------- ---------
9991001   ae10        1000     Access     413                   401                 26504                 828
9991002   te-1/1/5    1000     Access     2335                  3022                149440                204468
```

run clear vxlan statistics

The **run clear vxlan statistics** command clears traffic statistics of the VXLAN tunnel.

Command Syntax

run clear vxlan statistics [**vni** <*vni-id*>]

Parameter

Parameter	Description
vni <*vni-id*>	Optional. Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.

Usage Guidelines

If you want to obtain the latest statistics information, use this command to clear the past statistics information. When new packets coming, new statistics information is generated.

Example

- Clear traffic statistics of the VXLAN tunnel.

```
admin@Xorplus# run clear vxlan statistics
admin@Xorplus# commit
```

set vxlans udp-port

To configure the UDP destination port number for VXLAN, use the **set vxlans udp-port** command in L2/L3 configuration mode. The default VXLAN UDP port number is 4789.

Command Syntax

set vxlans udp-port <*number*>

Parameters

Parameter	Description
udp-port <*number*>	VXLAN UDP port number. The range of values is from 1024 to 65535.

Example

This example demonstrates how to configure the VXLAN UDP port association to 5000:

```
admin@XorPlus# set vxlans udp-port 5000
admin@XorPlus# commit
```

run show vxlan vni

Run the command **run show vxlan vni** to list all interfaces, their types and the associated egress and VLAN IDs for a specific VNI. Interface types includes Access, Network (unicast) and Network (multicast).

Command Syntax

run show vxlan vni <*vni-id*>

Parameter

Parameter	Description
vni <*vni-id*>	Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.

Example

- Show the VXLAN list of all interfaces, which includes the type, associated egress, VLAN ID, vtep and vplag of the specified VNI.

```
admin@PICOS# run show vxlan vni 10010
Interface      ID             Type           Egress     Vlan ID     Vtep               vplag
-----------    -----------    -----------    -------    --------    ---------------    --------
te-1/1/2       0x70000000     Access         100002     2
```

run show vxlan address-table

Run the command **run show vxlan address-table** to display the VXLAN address table on the switch. MAC addresses belonging to different VNI's are listed along with its type, interface and the associated VTEP.

Command Syntax

run show vxlan address-table

Parameter

None.

Example

- Show the information of VXLAN address table, including VNID, MAC address, type, interface and VTEP.

```
admin@SVNE3# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------    ---------------
99             04:f8:f8:20:67:7b    Dynamic                        10.226.14.254
99             18:5a:58:37:55:e1    Dynamic                        10.226.14.253
99             50:9a:4c:e6:7e:71    Dynamic                        10.226.14.201
10020          00:1e:c9:bb:c0:3c    Dynamic    ge-1/1/19
10020          04:f8:f8:20:67:7b    Dynamic                        10.226.14.254
10020          18:5a:58:37:55:e1    Dynamic                        10.226.14.253
10020          50:9a:4c:e6:7e:71    Dynamic                        10.226.14.201
10030          04:f8:f8:20:67:7b    Dynamic                        10.226.14.254
10030          18:5a:58:37:55:e1    Dynamic                        10.226.14.253
10030          22:00:00:00:00:00    Dynamic                        10.226.14.254
10030          50:9a:4c:e6:7e:71    Dynamic                        10.226.14.201
Entries in access port:  1
Entries in network port: 10
```

run show vxlan arp

The **run show vxlan arp** command can be used to display the local ARP entries of IPv4 address.

Command Syntax

run show vxlan arp

Parameter

None.

Example

- Show the local ARP entries of IPv4 address, including the local IPv4 address, MAC address, VNI, status, age, interface and the remote VTEP.

```
admin@SVNE2# run show vxlan arp
IP-ADDRESS       MAC-ADDRESS        VNI       Status   Age   Interface   VTEP/Nexthop-Group
---------------  -----------------  --------  -------  ----  ----------  ---------------
192.168.20.17    90:3c:b3:4c:af:f9  10020     Static                     10.226.14.201
192.168.20.24    50:9a:4c:e6:7e:71  10020     Static                     10.226.14.201
192.168.20.110   e4:f0:04:80:ea:cd  10020     Dynamic  546   ae2
192.168.20.135   8c:ea:1b:a8:c5:41  10020     Static                     10.226.14.201
192.168.30.17    90:3c:b3:4c:af:f9  10030     Static                     10.226.14.201
192.168.30.24    50:9a:4c:e6:7e:71  10030     Static                     10.226.14.201
192.168.30.110   e4:f0:04:80:ea:cd  10030     Dynamic  490   ae2
```

run show vxlan l3-vni entry

The **run show vxlan l3-vni entry** command can be used to display VXLAN information of Layer 3 VNIs, including interface ID, SVI (Switch Virtual Interface) interface, remote VTEP, neighbor router-MAC address and egress ID.

Command Syntax

run show vxlan l3-vni entry

Parameter

None.

Example

- Show the VXLAN information of all Layer 3 VNIs, including interface ID, SVI (Switch Virtual Interface) interface, remote VTEP, neighbor router-MAC address and egress ID.

```
admin@SVNE2# run show vxlan l3-vni entry
L3-VNI    Interface-Id   SVI-Interface  Remote-VTEP      Neighbor-RMAC      Egress-Id
--------  -------------  -------------  ---------------  -----------------  ---------
99        0x1800         vlan99         10.226.14.201    50:9a:4c:e6:7e:71  0x66a80
```

run show vxlan neighbor

The **run show vxlan neighbor** command can be used to display the local ARP entries of IPv6 address.

Command Syntax

run show vxlan neighbor

Parameter

None.

Example

- Show the ARP entries of IPv6 address, including the local IPv6 address, MAC address, VNI, status, age, interface and the remote VTEP.

```
admin@SVNE2# run show vxlan neighbor
IP-ADDRESS                                MAC-ADDRESS        VNI       Status   Age   Interface                 VTEP/Nexthop-Group
----------------------------------------  -----------------  --------  -------  ----  ----------  ------------------------
2002:0:0:1::17                            90:3c:b3:4c:af:f9  10020     Static                                 10.226.14.201
2002:0:0:1::24                            50:9a:4c:e6:7e:71  10020     Static                                 10.226.14.201
fe80::529a:4c20:3e6:7e71                  50:9a:4c:e6:7e:71  10020     Dynamic  204                           10.226.14.201
fe80::8eea:1b10:3a8:c541                  8c:ea:1b:a8:c5:41  10020     Dynamic  306                           10.226.14.201
fe80::923c:b320:14c:aff9                  90:3c:b3:4c:af:f9  10020     Dynamic  205                           10.226.14.201
fe80::aa2b:b510:1e0:94a7                  a8:2b:b5:e0:94:a7  10020     Dynamic  301   ae1
fe80::e6f0:418:180:eacd                   e4:f0:04:80:ea:cd  10020     Dynamic  301   ae2
2003:0:0:1::17                            90:3c:b3:4c:af:f9  10030     Static                                 10.226.14.201
2003:0:0:1::24                            50:9a:4c:e6:7e:71  10030     Static                                 10.226.14.201
fe80::529a:4c20:4e6:7e71                  50:9a:4c:e6:7e:71  10030     Dynamic  204                           10.226.14.201
fe80::923c:b320:24c:aff9                  90:3c:b3:4c:af:f9  10030     Dynamic  205                           10.226.14.201
```

set vxlans vni decapsulation mode

User can configure decapsulation mode for vxlan vni.

NOTE:

Trident3 platform switches do not support the following VXLAN commands:

set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add**

set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add-delete**

set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add-replace**

set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-delete**

set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-replace**

Command Syntax
set vxlans vni <*text*> **decapsulation mode** <*decapsulation-mode*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted format 100.100.200
mode <*decapsulation-mode*>	Configure vxlan tunnel encapsulation mode. Required select*ion* include: • **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged. • **service-vlan-add**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan, otherwise will be PVID of that port. • **service-vlan-add-delete**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan. Otherwise, it will be PVID of that port. From access to access, delete tag for tagged packets. • **service-vlan-add-replace**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan, otherwise will be PVID of that port. From access to access, replace tag for tagged packets. This is default value. • **service-vlan-delete**: From access to access, delete tag for tagged packets.

	• **service-vlan-replace**: From access to access, replace tag for tagged packets. • **service-vlan-per-port**: The decapsulated packet can be tagged or untagged dynamically based on the setting on the output port.

Example

• This example demonstrates how to configure the VXLAN tunnel decapsulation mode for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 decapsulation mode none
admin@XorPlus# commit
```

set vxlans vni encapsulation mode

User can configure encapsulation mode for vxlan vni.

NOTE:

Trident3 platform switches do not support the following VXLAN commands:

set vxlans vni <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add**

set vxlans vni <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add-delete**

set vxlans vni <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add-replace**

set vxlans vni <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-delete**

set vxlans vni <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-replace**

Command Syntax

set vxlans vni <*text*> **encapsulation mode** <*encapsulation-mode*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted format 100.100.200
mode<*encapsulation-mode*>	Configure vxlan tunnel encapsulation mode. Required select include: • **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged. • **service-vlan-add**: Add 802.1Q tag for untagged packets, and nothing changed with tagged packets. Encapsulation vlan is required. • **service-vlan-add-delete**: Add 802.1Q tag for untagged packets, and delete tag for tagged packets. Encapsulation vlan is required. • **service-vlan-add-replace**: Add 802.1Q tag for untagged packets, and replace tag for tagged packets. Encapsulation vlan is required. • **service-vlan-delete**: Delete 802.1Q tag for tagged packets, and nothing changed with untagged packets. This is default value according to RFC 7348. • **service-vlan-replace**: Replace vlan id of 802.1Q tag for tagged packets, and nothing changed with untagged packets. Encapsulation vlan is required.

Example

• This example demonstrates how to configure the VXLAN tunnel encapsulation mode for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 encapsulation mode none
admin@XorPlus# commit
```

set vxlans vni encapsulation vlan

User can configure flood vtep address for vxlan vni.

Command Syntax

set vxlans vni <*text*> **encapsulation vlan** <*vlan-id*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted format 100.100.200
vlan <*vlan-id*>	Add vlan id for vxlan tunnel encapsulation mode.

Example

• This example demonstrates how to configure the VXLAN tunnel encapsulation mode add vlan id for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 encapsulation vlan 100
admin@XorPlus# commit
```

set vxlans vni flood vtep

User can configure flood vtep address for vxlan vni.

Command Syntax
set vxlans vni <*text*> **flood vtep** <*ipv4-addr*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
vtep <*ipv4-addr*>	IPv4 address of vxlan vtep.

Example
• This example demonstrates how to configure the VXLAN head-end replication flood lists for the VNI 10010.

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1
XorPlus# set vxlans vni 10010 flood vtep 30.30.30.1
XorPlus# commit
```

set vxlans vni flood vtep mac-address

User can configure the flood vtep address set static mac address for vni.

Command Syntax

set vxlans vni <*text*> **flood vtep** <*ipv4-addr*> **mac-address** <*macaddr*>

delete vxlans vni <*text*> **flood vtep** <*ipv4-addr*> **mac-address** <*macaddr*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
vtep <*ipv4-addr*>	IPv4 address of vxlan vtep.
mac-address <*macaddr*>	Static mac address identifier.

Example

• This example demonstrates how to configure the VXLAN flood vtep address set static mac address is 00:e0:fc:00:0a:0b for the VNI

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1 mac-address 00:e0:fc:00:0a:0b
XorPlus# commit
```

set vxlans vni flood vtep traffic-type

User can configure the flood vtep address set forwarding traffic type for vni .

Command Syntax

set vxlans vni <*text*> **flood vtep** <*ipv4-addr*> **traffic-type** <*type-mode*>

delete vxlans vni <*text*> **flood vtep** <*ipv4-addr*> **traffic-type**

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
vtep <*ipv4-addr*>	IPv4 address of vxlan vtep.
traffic-type <*type-mode*>	Forwarding traffic type mode. Required select include: • **BUM** Transport BUM(broadcast, unknow unicast and multicast) traffic only • **all** Transport all traffic through this vtep, the default mode • **unicast** Transport known unicast traffic only

Example

• This example demonstrates how to configure the VXLAN flood vtep address set forwarding traffic type is BUM for the VNI 10010

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1 traffic-type BUM
XorPlus# commit
```

set vxlans vni vlan

User can configure mapping between VLAN to VXLAN VNI. Note that, there is a one-to-one mapping between a VXLAN VNI and a VLAN.

Command Syntax

set vxlans vni <*text*> **vlan** <*vlan-id*>

delete vxlans vni <*text*> **vlan** <*vlan-id*>

Parameters

Parameter	Description
vni <*text*>	VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
vlan <*vlan-id*>	VLAN tag identifier, the valid VLAN numbers range 1-4094.

Example

• This example demonstrates how to configure mapping between VLAN 100 to VXLAN VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 vlan 100
admin@XorPlus# commit
```

set vxlans tunnel-mac-leaning disable

User can configure disable VXLAN tunnels interface mac learning.

Command Syntax
set vxlans tunnel-mac-leaning disable <*boolean*>

delete vxlans tunnel-mac-leaning disable

Parameters

Parameter	Description
<*boolean*>	enable or disable VXLAN tunnels interface mac learning. • **true** disable VXLAN tunnels interface mac learning • **false** enable VXLAN tunnels interfaces mac learning

Example
• This example demonstrates how to configure disable VXLAN tunnels interface mac learning.

```
admin@XorPlus# set vxlans tunnel-mac-leaning disable true
admin@XorPlus# commit
```

set vxlans l3-vni

The command **set vxlans l3-vni** is used to add the L3 VNI ID to VXLAN routing. It will advertise the Type-2 host advertisements and Type-5 prefix routes for the VNI. The optional argument **prefix-routes-only** can be added to the command to advertise the prefix routes only. This configuration is used in EVPN Asymmetric routing to sync external routes between devices.

Run the command **delete vxlans l3-vni** to remove this configuration from the system.

Command Syntax

set vxlans [vrf <*vrf-name***>] l3-vni <***vni-id***> [prefix-routes-only]**

delete vxlans [vrf <*vrf-name***>] l3-vni <***vni-id***> [prefix-routes-only]**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional, specifies the VRF name.
l3-vni <*vni-id*>	Specifies the layer 3 VNI ID.

Example

This example demonstrates how to enable advertisement of Type-2 and Type-5 routes for a given VRF and VNI ID.

```
admin@XorPlus# set vxlans vrf vrf1 l3-vni 100
admin@XorPlus# commit
```

BGP EVPN Commands

- run show bgp evpn summary
- run show bgp evpn import-rt
- run show bgp evpn vrf-import-rt
- run show bgp evpn vni
- run show evpn es
- run show evpn access-vlan
- run show evpn arp-cache
- run show evpn next-hops
- run show evpn rmac
- run show evpn mac vni
- set interface aggregate-ethernet evpn mh es-df-pref
- set interface aggregate-ethernet evpn mh es-id
- set interface aggregate-ethernet evpn mh es-sys-mac
- set l3-interface routed-interface router-mac
- set l3-interface vlan-interface anycast address
- set l3-interface vlan-interface anycast mac
- set l3-interface vlan-interface router-mac
- set protocols bgp evpn advertise-default-gw
- set protocols bgp evpn advertise ipv4-unicast
- set protocols bgp evpn advertise ipv6-unicast
- set protocols bgp evpn advertise-svi-ip
- set protocols bgp evpn default-originate
- set protocols bgp evpn disable-ead-evi-rx
- set protocols bgp evpn disable-ead-evi-tx
- set protocols bgp evpn vni
- set protocols bgp evpn vni advertise-default-gw
- set protocols bgp evpn vni advertise-svi-ip
- set protocols bgp evpn vni rd
- set protocols bgp evpn vni route-target type
- set protocols bgp neighbor evpn activate
- set protocols bgp neighbor evpn allowas-in
- set protocols bgp neighbor evpn route-map
- set protocols bgp neighbor evpn route-reflector-client
- set protocols bgp vrf evpn advertise-pip ip
- set protocols evpn mh mac-holdtime
- set protocols evpn mh redirect-off
- set protocols evpn mh startup-delay
- set vxlans vni arp-nd-suppress disable
- set protocols bgp evpn advertise-all-vni
- set protocols evpn mh neigh-holdtime
- run show bgp evpn route
- run show bgp evpn route detail
- run show bgp evpn route vni
- run show bgp evpn route rd
- run show bgp evpn route type

run show bgp evpn summary

Run the command **run show bgp evpn summary** to display some basic information related to BGP EVPN. The output includes BGP router ID, local AS number, VRF membership and peer count etc. The output also includes a brief display of BGP EVPN packet statistics such as messages sent/received and router ID of remote peer.

Command Syntax

run show bgp evpn summary

Example

- Configure BGP EVPN to disable BUM traffic.

```
admin@Xorplus# run show bgp evpn summary
BGP router identifier 1.1.1.1, local AS number 65001 vrf-id 0
BGP table version 0
RIB entries 3, using 576 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
2.2.2.2         4      65001         9         8        0    0    0 00:03:16            2

Total number of neighbors 1
```

run show bgp evpn import-rt

The **run show bgp evpn import-rt** command displays VNI lists of all importing route target.

Command Syntax

run show bgp evpn import-rt

Example

- Display VNI lists of all importing route target.

```
admin@SVNE2# run show bgp evpn import-rt
Route-target: 0:10020
List of VNIs importing routes with this route-target:
  10020
Route-target: 0:10030
List of VNIs importing routes with this route-target:
  10030
```

run show bgp evpn vrf-import-rt

Run the command **run show bgp evpn vrf-import-rt** to display VRF lists with specified route target and import type.

Command Syntax

run show bgp evpn vrf-import-rt

Example

- Display VRF lists with specified route target and import type.

```
admin@SVNE2# run show bgp evpn vrf-import-rt
Route-target: 0:99
List of VRFs importing routes with this route-target:
  vrf1
```

run show bgp evpn vni

Run the command **run show bgp evpn vni** to display EVPN VNI related information. The output displays information such as VXLAN VNI gateway MAC-IP advertisement is enabled or not, SVI MAC-IP advertisement enabled or disabled. Also if advertisement of all VNIs is enabled or not. Other information displayed includes VNI ID, Type, RD, Import RT, Export RT and Tenant VRF.

Command Syntax

run show bgp evpn vni

Example

- Display BGP EVPN VNI information.

```
admin@Xorplus# run show bgp evpn vni
Advertise Gateway Macip: Disabled
Advertise SVI Macip: Disabled
Advertise All VNI flag: Enabled
BUM flooding: Head-end replication
Number of L2 VNIs: 1
Number of L3 VNIs: 0
Flags: * - Kernel
  VNI        Type RD                  Import RT              Export RT              Tenant VRF
* 10         L2   1.1.1.1:2           65001:10               65001:10               default
```

run show evpn es

The **run show evpn es** command is used to display the all the Ethernet segments configured on the device. It also displays the auto generated type-3 ESI for each segment, its type, the name of the LAG interface and the VTEPs involved.

Example:

```
admin@ACC2# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                               Type      ES-IF                 VTEPs
03:00:22:22:22:22:22:00:00:01      LR        ae1                  10.226.14.253,10.226.14.254
03:00:22:22:22:22:22:00:00:02      LR        ae2                  10.226.14.253,10.226.14.254
```

To check the detailed information of the Ethernet segments, add the optional keyword detail at the end of the command as shown below.

```
admin@ACC2# run show evpn es detail
ESI: 03:00:22:22:22:22:22:00:00:01
 Type: Local,Remote
 Interface: ae1
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
 DF status: df
 DF preference: 32767
 Nexthop group: 536870913
 VTEPs:
     10.226.14.253 df_alg: preference df_pref: 32767 nh: 268435459
     10.226.14.254 df_alg: preference df_pref: 32767 nh: 268435460


ESI: 03:00:22:22:22:22:22:00:00:02
 Type: Local,Remote
 Interface: ae2
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
 DF status: df
 DF preference: 32767
 Nexthop group: 536870914
 VTEPs:
     10.226.14.253 df_alg: preference df_pref: 32767 nh: 268435459
     10.226.14.254 df_alg: preference df_pref: 32767 nh: 268435460
```

run show evpn access-vlan

The **run show evpn access-vlan** command is used to view the EVPN information of specified access VLAN.

Command Syntax

run show evpn access-vlan [<*vlan-id*> | **detail**]

Parameters

Parameter	Description
<*vlan-id*>	VLAN tag identifier, the valid VLAN numbers range 1-4094.

Example

- View the EVPN information of access VLAN 99.

```
admin@SVNE2# run show evpn access-vlan 99
VLAN: 99
 VxLAN Interface: vxlan99
 SVI: vlan99
 L2-VNI: 0
 Member Count: 0
 Members:
```

- View the EVPN information of all access VLANs.

```
admin@SVNE2# run show evpn access-vlan
VLAN  SVI             L2-VNI   VXLAN-IF        # Members
99    vlan99          0        vxlan99         0
20    vlan20          10020    vxlan10020      3
30    vlan30          10030    vxlan10030      3
4094  vlan4094        0        -               1
1     -               0        -               3
```

- View the detailed EVPN information of all access VLANs.

```
admin@SVNE2# run show evpn access-vlan detail
VLAN: 99
 VxLAN Interface: vxlan99
 SVI: vlan99
 L2-VNI: 0
 Member Count: 0
 Members:

VLAN: 20
 VxLAN Interface: vxlan10020
 SVI: vlan20
 L2-VNI: 10020
```

```
 Member Count: 3
 Members:
    ae1
    ae2
    ae24

VLAN: 30
 VxLAN Interface: vxlan10030
 SVI: vlan30
 L2-VNI: 10030
 Member Count: 3
 Members:
    ae1
    ae2
    ae24
```

run show evpn arp-cache

The **run show evpn arp-cache** command can be used to display the local ARP entries of IPv4 and IPv6 address belonging to specified VNI ID.

Command Syntax

run show evpn arp-cache vni [*<vni>* | **all**]

Parameters

Parameter	Description
<vni>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- Display the local ARP entries of IPv4 and IPv6 address belonging to VNI 10020.

```
admin@SVNE2# run show evpn arp-cache vni 10020
Number of ARPs (local and remote) known for this VNI: 15
Flags: I=local-inactive, P=peer-active, X=peer-proxy
Neighbor                 Type   Flags State    MAC               Remote ES/VTEP
Seq #'s
192.168.20.135           remote       active   8c:ea:1b:a8:c5:41 10.226.14.201
0/0
192.168.20.24            remote       active   50:9a:4c:e6:7e:71 10.226.14.201
0/0
192.168.20.17            remote       active   90:3c:b3:4c:af:f9 10.226.14.201
0/0
fe80::6f8:f810:120:677b  local        inactive 04:f8:f8:20:67:7b
0/0
192.168.20.47            local        active   18:5a:58:37:55:e1
0/0
2002:0:0:1::47           local        active   18:5a:58:37:55:e1
0/0
fe80::8eea:1b10:3a8:c541 remote       active   8c:ea:1b:a8:c5:41 10.226.14.201
0/0
192.168.20.110           local        active   e4:f0:04:80:ea:cd
0/0
fe80::529a:4c20:3e6:7e71 remote       active   50:9a:4c:e6:7e:71 10.226.14.201
0/0
fe80::aa2b:b510:1e0:94a7 local        inactive a8:2b:b5:e0:94:a7
0/0
2002:0:0:1::24           remote       active   50:9a:4c:e6:7e:71 10.226.14.201
0/0
fe80::e6f0:418:180:eacd  local        active   e4:f0:04:80:ea:cd
0/0
fe80::923c:b320:14c:aff9 remote       active   90:3c:b3:4c:af:f9 10.226.14.201
0/0
```

```
2002:0:0:1::17           remote       active   90:3c:b3:4c:af:f9 10.226.14.201
0/0
fe80::1a5a:5810:137:55e1 local        active   18:5a:58:37:55:e1
0/0
```

run show evpn next-hops

The **run show evpn next-hops** command can be used to view the EVPN next-hop information belonging to specified VNI ID.

Command Syntax

run show evpn next-hops vni <*vni*>

Parameters

Parameter	Description
<*vni*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- View the EVPN next-hop information belongding to VNI 99.

```
admin@SVNE2# run show evpn next-hops vni 99
Number of NH Neighbors known for this VNI: 2
IP              RMAC
::ffff:ae2:ec9  90:3c:b3:4c:af:f9
10.226.14.201   90:3c:b3:4c:af:f9
```

run show evpn rmac

The **run show evpn rmac** command is used to view the router MAC address corresponding to all remote VTEPs belonging to specified VNIs.

Command Syntax

run show evpn rmac vni <*vni*>

Parameters

Parameter	Description
<*vni*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- View the router MAC address corresponding to all remote VTEPs belonging to VNI 99.

```
admin@SVNE2# run show evpn rmac vni 99
Number of Remote RMACs known for this VNI: 2
MAC               Remote VTEP
90:3c:b3:4c:af:f9 10.226.14.201
50:9a:4c:e6:7e:71 10.226.14.201
```

run show evpn mac vni

Run the command **run show evpn mac vni** to display all the MAC addresses learned on different interfaces belonging to a particular VNI. It also shows whether the MAC is learned locally or remotely and shows the associated VLAN.

Example:

```
admin@SVNE3# run show evpn mac vni 10030
Number of MACs (local and remote) known for this VNI: 5
Flags: N=sync-neighs, I=local-inactive, P=peer-active, X=peer-proxy
MAC               Type   Flags Intf/Remote ES/VTEP           VLAN  Seq #'s
22:00:00:00:00:00 remote       10.226.14.254                       0/0
18:5a:58:37:55:e1 remote       10.226.14.253                       0/0
50:9a:4c:e6:7e:71 remote       10.226.14.201                       0/0
18:5a:58:37:64:61 local        vlan30                        30    0/0
04:f8:f8:20:67:7b remote       10.226.14.254                       0/0
```

set interface aggregate-ethernet evpn mh es-df-pref

Run the command **set interface aggregate-ethernet evpn mh es-df-pref** to set the preference value used in the Designated Forwarder (DF) election process on a given aggregate Ethernet interface. The default value of DF preference is 32767. If there is a tie between the nodes over the preference value then the VTEP with the smallest IP address wins the election.

Please note that DF preference can only be set for an aggregate Ethernet interface.

Run the command **delete interface aggregate-ethernet evpn mh es-df-pref** to remove this configuration from the switch.

Command Syntax

set interface aggregate-ethernet <*interface*> **evpn mh es-df-pref <***preference***>**

delete interface aggregate-ethernet <*interface*> **evpn mh es-df-pref**

Parameter

Parameter	Description
aggregate-ethernet <*interface*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-df-pref <*preference***>**	Specifies the Ethernet segment DF preference, the value is an integer that ranges from 1 to 65535. The default value is 32767.

Example

- Configure the DF preference value to 45000.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-df-pref 45000
admin@Xorplus# commit
```

set interface aggregate-ethernet evpn mh es-id

Run the command **set interface aggregate-ethernet evpn mh es-id** to set the Ethernet Segment Identifier (ES-ID) for the EVPN multi-homing feature on a given aggregate Ethernet interface.

Run the command **delete interface aggregate-ethernet evpn mh es-id** to delete the ES-ID from the switch configuration.

Command Syntax

set interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-id <***ES-ID***>**

delete interface aggregate-ethernet <*aggregate-ethernet***> evpn mh es-id**

Parameter

Parameter	Description
aggregate-ethernet <*aggregate-ethernet*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-id <*ES-ID*>	Specifies the ES-ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the ES-ID to 40 for aggregate Ethernet interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-id 40
admin@Xorplus# commit
```

set interface aggregate-ethernet evpn mh es-sys-mac

Run the command **set interface aggregate-ethernet evpn mh es-sys-mac** to configure the EVPN multi-homing Ethernet Segment System MAC address on a given aggregate Ethernet interface.

Run the command **delete set interface aggregate-ethernet evpn mh es-sys-mac** to delete this configuration from the switch.

Command Syntax

set interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-sys-mac <***system-mac***>**

delete interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-sys-mac**

Parameter

Parameter	Description
aggregate-ethernet <*aggregate-ethernet*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-sys-mac <*system-mac***>**	Specifies the Ethernet segment system MAC address, the value is in 48 bit hexadecimal MAC address format, e.g. 00:22:22:22:22:22

Example

- Configure the EVPN multi-homing Ethernet segment system MAC for interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Xorplus# commit
```

set l3-interface routed-interface router-mac

The **set l3-interface routed-interface router-mac** command sets the router MAC address of the anycast gateway on a routed interface or sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **router-mac** <*macaddr*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
router-mac <*macaddr*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the router MAC address of the anycast gateway on a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te3 router-mac 00:00:10:00:00:FE
admin@Xorplus# commit
```

set l3-interface vlan-interface anycast address

The **set l3-interface vlan-interface anycast address** command configures the virtual IP address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **anycast address** <*ip-address*> **prefix-length** <*prefix*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies the L3 VLAN interface. The value is a string.
address <*ip-address*>	Specifies IPv4 or IPv6 address.
prefix-length <*prefix*>	Specifies the network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Usage Guidelines

Follow the rules below when configuring the anycast IPv4 / IPv6 address:

- For IPv4, the anycast IPv4 address and the VLAN interface IPv4 address should be configured in the same network segment to ensure that the MLAG pair can work normally.
- For IPv6, the anycast IPv6 address and the global IPv6 address of the VLAN interface should be configured in the same network segment to ensure that the MLAG pair can work normally.
- Anycast IP address list on both devices of MLAG pair must be the same.
- When configuring the **Anycast MAC** and **Anycast Address** for an L3 interface, it is necessary to apply both configurations in the same **commit**. This is because these two settings are interdependent, and applying them separately might cause synchronization issues, leading to configuration failures or network instability.

Example

- Configure the virtual IP address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast address 10.0.1.1 prefix-length 24
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast mac AE:00:10:00:00:FE
admin@Xorplus# commit
```

set l3-interface vlan-interface anycast mac

> **NOTE:**
> When configuring the **Anycast MAC** and **Anycast Address** for an L3 interface, it is necessary to apply both configurations in the same **commit**. This is because these two settings are interdependent, and applying them separately might cause synchronization issues, leading to configuration failures or network instability.

The **set l3-interface vlan-interface anycast mac** command configures the virtual MAC address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **anycast mac** <*mac-address*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies the L3 VLAN interface. The value is a string.
mac <*mac-address*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the virtual MAC address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast address 10.0.1.1 prefix-length 24
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast mac AE:00:10:00:00:FE
admin@Xorplus# commit
```

set l3-interface vlan-interface router-mac

The **set l3-interface vlan-interface router-mac** command configures the router MAC address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*vlan-interface-name*> **router-mac** <*macaddr*>

Parameter

Parameter	Description
vlan-interface <*vlan-interface-name*>	Specifies the L3 VLAN interface. The value is a string.
router-mac <*macaddr*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the router MAC address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 router-mac 00:00:10:00:00:FE
admin@Xorplus# commit
```

set protocols bgp evpn advertise-default-gw

The **set protocols bgp evpn advertise-default-gw** command is used to configure the gateway VTEPs to advertise the IP/MAC address. Optional parameter **vrf** can be added to identify the VRF for which to advertise the IP/MAC address.

The **delete protocols bgp evpn advertise-default-gw** can be used to delete the configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn advertise-default-gw**

delete protocols bgp [vrf <*vrf-name*>**] evpn advertise-default-gw**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure BGP EVPN to advertise default gateway for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn advertise-default-gw
admin@Xorplus# commit
```

set protocols bgp evpn advertise ipv4-unicast

The **set protocols bgp evpn advertise ipv4-unicast** command is used to announce IPv4 prefixes in the BGP RIB as EVPN Type-5 routes. Add the optional parameter **route-map** if you want to add a route map filter to the IPv4 Type-5 route advertisement. If the route map filter is not used, all the IPv4 routes in the BGP RIB are included in the advertisement. Optional parameter **vrf** can be used if you want the command to take effect on a specific VRF.

The **delete protocols bgp evpn advertise ipv4-unicast** command can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf *<vrf-name>]* **evpn advertise ipv4-unicast [route-map** *<route-map>***]**

delete protocols bgp [vrf <*vrf-name***>] evpn advertise ipv4-unicast [route-map** *<route-map>***]**

Parameter

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies the name of the VRF name. The value is a string.
route-map *<route-map>*	Optional. Specifies the route-map to filter the Type-5 IPv4 routes while advertising. The value is a string.

Example

- Configure the device to announce the IPv4 prefixes in VRF BLUE for EVPN and apply the map1 route-map filter.

```
admin@Xorplus# set protocols bgp vrf BLUE advertise ipv4-unicast route-map map1
admin@Xorplus# commit
```

set protocols bgp evpn advertise ipv6-unicast

The command **set protocols bgp evpn advertise ipv6-unicast** is used to configure the device to announce IPv6 prefixes in the BGP RIB as EVPN Type-5 routes. Add the optional parameter **route-map** if you want to add a route map filter to the IPv6 Type-5 route advertisement. If the route map filter is not used, all the IPv6 routes in the BGP RIB are included in the advertisement. The other optional parameters are **vrf** to specify a VRF for this command to take effect on.

To delete this configuration, run the command **delete set protocols bgp evpn advertise ipv6-unicast.**

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn advertise ipv6-unicast [route-map** <*route-map*>**]**

delete protocols bgp [vrf <*vrf-name***>] evpn advertise ipv6-unicast [route-map** <*route-map*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
route-map <*route-map*>	Specifies a route map filter for the IPv6 Type-5 route advertisement. The value is a string.

Example

- Configure the device to advertise EVPN Type-5 IPv6 routes in VRF BLUE and apply route-map map1.

```
admin@Xorplus# set protocols bgp vrf BLUE advertise ipv6-unicast route-map map1
admin@Xorplus# commit
```

set protocols bgp evpn advertise-svi-ip

Run the command **set protocols bgp evpn advertise-svi-ip** to advertise the local SVI IP address so that it can be accessible from remote VTEPs. This command is needed when unique SVIs are used across different racks. You should not use this command if SVI addresses are reused across different racks and are not unique.

Run the command **delete protocols bgp evpn advertise-svi-ip** to remove this configuration.

Command Syntax

set protocols bgp evpn advertise-svi-ip

delete protocols bgp evpn advertise-svi-ip

Example

- Configure the device to advertise the local SVI IP.

```
admin@Xorplus# set protocols bgp evpn advertise-svi-ip
admin@Xorplus# commit
```

set protocols bgp evpn default-originate

To enable originating a default Type-5 route, run the command **set protocols bgp evpn default-originate**. Both the IPv4 and IPv6 default Type-5 routes are supported to be originated. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp evpn default-originate** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn default-originate** <**ipv4 | ipv6>**

delete protocols bgp [vrf <*vrf-name*>**] evpn default-originate <ipv4 | ipv6**>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
default-originate <ipv4|ipv6>	Specifies whether IPv4 or IPv6 Type-5 route to be originated.

Example

- Configure the device to originate the IPv4 default Type-5 routes for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn default-originate ipv4
admin@Xorplus# commit
```

set protocols bgp evpn disable-ead-evi-rx

Some implementations of EVPN do not advertise EAD-per-EVI routes so to be compatible with these vendors; we need to manually disable advertisement of EAD-per-EVI routes. To activate the VTEP upon receiving EAD-per-ES route and suppress the dependency on EAD-per-EVI routes, run the command **set protocols bgp evpn disable-ead-evi-rx.**

Optional parameter **vrf** can be used to identify a specific VRF for this command to take effect on.

The command **delete protocols bgp evpn disable-ead-evi-rx** can be used to remove this configuration.

Command Syntax

set protocol bgp [vrf <*vrf-name***>] evpn disable-ead-evi-rx**

delete protocol bgp [vrf <*vrf-name***>] evpn disable-ead-evi-rx**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure the device to disable EVPN advertisement of EAD-per-EVI routes in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn disable-ead-evi-rx
admin@Xorplus# commit
```

set protocols bgp evpn disable-ead-evi-tx

Since the Type-1/EAD (Ethernet Auto Discovery) routes are to be advertised in the following two ways as per RFC 7432:

1. Ethernet Auto Discovery per Ethernet Segment (EAD-per-ES) routes
2. Ethernet Auto Discovery per EVPN Instance (EAD-per-EVI) routes

Some implementations of EVPN don't advertise EAD-per-EVI routes so to be compatible with these vendors; we need to manually disable advertisement of EAD-per-EVI routes.
To suppress the advertisement of EAD-per-EVI routes, run the command **set protocols bgp evpn disable-ead-evi-tx.** Optional parameter **vrf** can be used to identify a specific VRF for this command to take effect on.

To delete this configuration, run the command **delete protocols bgp evpn disable-ead-evi-tx.**

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn disable-ead-evi-tx**

delete protocols bgp [vrf <*vrf-name***>] evpn disable-ead-evi-tx**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure the device to disable EVPN advertisement of EAD-per-EVI routes in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn disable-ead-evi-tx
admin@Xorplus# commit
```

set protocols bgp evpn vni

To add a VXLAN VNI to BGP EVPN routing, run the command **set protocols bgp evpn vni**. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp evpn vni** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*>

delete protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni*>	Specifies the VNI to add to the BGP EVPN routing. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the device to add VNI 20 to EVPN BGP routing in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn vni 20
admin@Xorplus# commit
```

set protocols bgp evpn vni advertise-default-gw

Run the command **set protocols bgp evpn vni advertise-default-gw** to configure the gateway VTEPs to advertise their IP/MAC routes for the specified VNI. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

Run the command **delete protocols bgp evpn vni advertise-default-gw** to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-default-gw**

delete protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-default-gw**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni*>	Specifies the VNI for which to advertise the default gateway.

Example

- Configure the device to advertise the default gateway in VRF BLUE for VNI 20.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn vni 20 advertise-default-gw
admin@Xorplus# commit
```

set protocols bgp evpn vni advertise-svi-ip

To advertise the local SVI IP address behind a specific VNI, run the command **set protocols bgp evpn vni advertise-svi-ip**.

To delete the configuration, run the command **delete protocols bgp evpn vni advertise-svi-ip.**

Command Syntax

set protocols bgp evpn vni <*vni*> **advertise-svi-ip**

delete protocols bgp evpn vni <*vni*> **advertise-svi-ip**

Parameter

Parameter	Description
vni <*vni*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the device to advertise the local SVI IP behind VNI 20.

```
admin@Xorplus# set protocols bgp evpn vni 20 advertise-svi-ip
admin@Xorplus# commit
```

set protocols bgp evpn vni rd

Run the command **set protocols bgp evpn vni rd** if you do not want that route distinguisher (RD) to be automatically derived and define them manually.

Run the command **delete protocols bgp evpn vni rd** to delete this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **rd** <*rd*>

delete protocol bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **rd** <*rd*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni-id*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.
rd <*rd*>	Specifies the route distinguisher. The value follows the format *RouterID:VNI-Index.*

Usage Guidelines

When the switch learns about a local VNI and there is no configuration available in the system regarding this VNI then the import and export route targets (RTs) and route distinguisher (RD) for this VNI will be automatically calculated. The RTs are automatically derived as *AS:VNI,* whereas RD is derived as *Router-ID:VNI-Index.*

For Type-2 and Type-3 routes coming from the layer 2 VNI, the RD is calculated as *VXLAN-local0-tunnelip:VNI* instead of *Router-ID:VNI.* Since EVPN routes may have the same MAC and/or the IP address; RDs are used to remove ambiguity in such cases. RTs are used to identify the VPN membership of routes.

Example

- Configure RD for VNI 20.

```
admin@Xorplus# set protocols bgp evpn vni 20 rd 10.1.1.1:20
admin@Xorplus# commit
```

set protocols bgp evpn vni route-target type

If we want the route target (RT) to be configured manually instead of being auto-configured, run the command **set protocols bgp evpn vni route-target type.** The command specifies the route target and its type as well. Parameter **type** can have three possible values, **export**, **import** or **both**. If you choose **both** then the RT can be used as both an import and export route target.

Run the command **delete protocols bgp evpn vni route-target** to delete this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **route-target** <*route-target*> **type <both | export | import>**

delete protocols bgp [vrf <*vrf-name***>] evpn vni** <*vni-id*> **route-target** <route-target> **type <both | export | import>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni-id*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.
route-target <*route-target*>	Specifies the route target. The value of route target follows the format *AS:VNI,* e.g. 65100:20
type <both | export | import>	Specifies the RT type as either import, export or both.

Example

- Configure the route target value 65100:20 for VNI 20 and apply this RT for both export and import of routes.

```
admin@Xorplus# set protocols bgp evpn vni 20 route-target 65100:20 type both
admin@Xorplus# commit
```

set protocols bgp neighbor evpn activate

Run the command **set protocols bgp neighbor evpn activate** to enable or disable the BGP peer within the EVPN address family to enable EVPN route exchange with the specified BGP peer.

Optional parameter **vrf** can be used to identify a VRF, if not defined, the command takes effect on the default VRF.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn activate <true | false>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
activate <true | false>	Enables or disables the address family for the specified neighbor • **true:** Enables the address family for the specified neighbor. • **false:** Disables the address family for the specified neighbor.

Example

- Configure the device to enable EVPN BGP route exchange with peer 3.3.3.3 in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn activate true
admin@Xorplus# commit
```

set protocols bgp neighbor evpn allowas-in

To allow BGP route updates from peers with the same AS number as the current system AS; run the command **set protocol bgp neighbor evpn allowas-in**. This configuration is needed when different BGP peers reside in different locations that cannot be directly connected but they both use the same AS number. Parameter **vrf** is optional and if not specified then the command will affect the default VRF.

The parameter value **<1-10>** configures the number of accepted occurrences of the current system AS number in AS path.

The parameter **origin** configures BGP to only accept routes originated with the same AS number as that of the current system.

Run the command **delete protocols bgp neighbor evpn allowas-in** to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn allowas-in {**<1-10> | **origin}**

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn allowas-in {**<1-10> | **origin}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
allowas-in {<1-10>	**origin}**	Value **<1-10>** specifies the number of occurrences of AS in AS path, **origin** configures BGP to only accept routes originated with the same AS number as that of the system.

Example

- Configure BGP to accept BGP EVPN route updates from peer 3.3.3.3 in VRF BLUE and also the accepted routes originated with the same AS number as the system.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn allowas-in origin
admin@Xorplus# commit
```

set protocols bgp neighbor evpn route-map

Run the command **set protocols bgp neighbor evpn route-map** to configure an inbound or outbound route map for an EVPN neighbor. The parameter value of neighbor is the BGP neighbor for which to specify the route map. The value of parameter route-map is where you specify the name of the route map to apply and keywords **in** or **out** are to specify whether the route map applies to inbound or outbound traffic. Optional parameter **vrf** can be used to specify a VRF. If VRF is not specified then the command applies to the default VRF.

The command **delete protocols bgp neighbor evpn route-map** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn {in | out} route-map** <*route-map*>

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn {in | out} route-map** <*route-map*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
in|out	Keywords to specify the inbound or outbound direction for route map.
route-map <*route-map*>	Specifies the name of the route map.

Example

- Configure to apply route map *map1* to for EVPN BGP peer 3.3.3.3 in the inbound direction for the VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn in route-map map1
admin@Xorplus# commit
```

set protocols bgp neighbor evpn route-reflector-client

Run the command **set protocols bgp neighbor evpn route-reflector-client** to configure the BGP node to act as a route reflector for the specified BGP peer for EVPN. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp neighbor evpn route-reflector-client** can be used to delete this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn route-reflector-client**

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn route-reflector-client**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example

- Configure the BGP to act as route reflector for the specified BGP peer for EVPN in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn route-reflector-client
admin@Xorplus# commit
```

set protocols bgp vrf evpn advertise-pip ip

Run the command **set protocols bgp vrf evpn advertise-pip ip** to advertise the Primary IP Address (PIP) for a given VRF. Parameter **vrf** is optional and if not defined then the command takes effects on the default VRF. We can specify a specific IP address to advertise by adding **ip** <*ipv4*>.

The **delete protocols bgp vrf evpn advertise-pip ip** can be used to delete this configuration.

Command Syntax

set protocols bgp vrf <*vrf-name*> **evpn advertise-pip ip** <*ipv4*>

delete protocols bgp vrf <*vrf-name*> **evpn advertise-pip ip** <*ipv4*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF. The value is a string.
ip <*ipv4*>	Specifies the IPv4 address to advertise. The value is a string in IPv4 dotted decimal format.

Example

- Configure BGP EVPN to advertise PIP 10.1.1.1 for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn advertise-pip ip 10.1.1.1
admin@Xorplus# commit
```

set protocols evpn mh mac-holdtime

Run the command **set protocols evpn mh mac-holdtime** to configure the EVPN MH MAC hold time in seconds. This is the length of time for which a device maintains the SYNC MAC entries after the Ethernet segment (ES) peer's type-2 route is deleted. The device will try and attempt to establish reachability with MAC on the local ES during this time. The MAC hold time ranges from 0 to 86400 and the default value is 1080 seconds.

Run the command **delete protocols evpn mh mac-holdtime** to delete this configuration.

Note: This is a global configuration and affects the MH configuration on the whole device.

Command Syntax

set protocols evpn mh mac-holdtime *<seconds>*

delete protocols evpn mh mac-holdtime

Parameter

Parameter	Description
mac-holdtime *<seconds>*	Specifies the MAC hold time in seconds, the range is from 0 to 86400. The default value is 1080 seconds.

Example

- Configure the EVPN MH MAC hold time to 234 seconds.

```
admin@Xorplus# set protocols evpn mh mac-holdtime 234
admin@Xorplus# commit
```

set protocols evpn mh redirect-off

Run the command **set protocols evpn mh redirect-off** to disable fast failover of traffic destined to the access port via the VXLAN overlay.

Run the command **delete protocols evpn mh redirect-off** to remove this configuration and enable fast failover of traffic.

Note: This is a global configuration and affects the whole device.

Command Syntax

set protocols evpn mh redirect-off

delete protocols evpn mh redirect-off

Example

- Disable fast failover of traffic.

```
admin@Xorplus# set protocols evpn mh redirect-off
admin@Xorplus# commit
```

set protocols evpn mh startup-delay

Run the command **set protocols evpn mh startup-delay** to configure the duration of time for which the device keeps the EVPN multihoming LAG interfaces in protocol down state after a device reboot or process restart. This delays allows the VXLAN overlay to complete its initialization and helps in a smooth operation.

Run the command **delete protocols evpn mh startup-delay** to remove this configuration and revert to default which is 180 seconds.

Command Syntax

set protocols evpn mh startup-delay <*seconds*>

delete protocols evpn mh startup-delay

Parameter

Parameter	Description
startup-delay <*seconds*>	Specifies the startup-delay in seconds. The value ranges from 0 to 36000, the default value is 180 seconds.

Example

- Set the startup-delay to 200 seconds.

```
admin@Xorplus# set protocols evpn mh startup-delay 200
admin@Xorplus# commit
```

set vxlans vni arp-nd-suppress disable

The **set vxlans vni arp-nd-suppress disable** command is used to enable or disable ARP/ND suppression function in MP-BGP EVPN networks.

Command Syntax

set vxlans vni <*vni-id*> **arp-nd-suppress disable <true | false>**

Parameter

Parameter	Description
vni <*vni-id*>	Specifies the L2 VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.
disable <true | false>	Enable or disable ARP/ND suppression function. The value could be **true** or **false**. • **true**: Disable ARP/ND suppression. • **false**: Enable ARP/ND suppression. By default, ARP/ND suppression is disabled.

Example

- Enable ARP/ND suppression function.

```
admin@Xorplus# set vxlans vni 10010 arp-nd-suppress disable false
admin@Xorplus# commit
```

set protocols bgp evpn advertise-all-vni

The **set protocols bgp evpn advertise-all-vni** command is used to enable the BGP control plane for all VNIs configured on the switch in the default VRF.

Note that only leaf switches that are VTEPs need this configuration.

The **delete protocols bgp evpn advertise-all-vni** command can be used to delete this configuration.

Command Syntax

set protocols bgp evpn advertise-all-vni

delete protocols bgp evpn advertise-all-vni

Example

- Configure BGP EVPN to advertise all VNIs in the default VRF.

```
admin@Xorplus# set protocols bgp evpn advertise-all-vni
admin@Xorplus# commit
```

set protocols evpn mh neigh-holdtime

Run the command **set protocols evpn mh neigh-holdtime** to configure the neighbor entry hold time in seconds. The device will maintain the SYNC neighbor entries during this time after the ES peer's EVPN type-2 route is deleted. The device independently tries to establish reachability with the MAC/host on the local ES during this time period.

Run the command **delete protocols evpn mh neigh-holdtime** to delete this configuration and revert back to the default value which is 1080 seconds.

Note: This is a global EVPN MH configuration and affects the whole device.

Command Syntax

set protocols evpn mh neigh-holdtime <*seconds*>

delete protocols evpn mh neigh-holdtime

Parameter

Parameter	Description
neigh-holdtime <*seconds*>	Specifies the neighbor entry hold time in seconds. The value ranges from 0 to 86400. The default value is 1080 seconds.

Example

- Configure the EVPN MH neighbor entry hold time to 234 seconds.

```
admin@Xorplus# set protocols evpn mh neigh-holdtime 234
admin@Xorplus# commit
```

run show bgp evpn route

Run the command **run show bgp evpn route** to display all BGP EVPN routes in the routing table.

Command Syntax

run show bgp evpn route

Parameters

None.

Example

- Display all BGP EVPN routes.

```
admin@51.134# run show bgp evpn route
   Network          Next Hop            Metric LocPrf Weight Path
                    Extended Community
Route Distinguisher: 134.134.134.134:2
*> [5]:[0]:[24]:[33.1.1.0]
                    134.134.134.134          0         32768 i
                    ET:8 RT:134:9999 Rmac:04:f8:f8:20:6c:7b
Route Distinguisher: 134.134.134.134:3
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:22221
Route Distinguisher: 134.134.134.134:4
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:22222
Route Distinguisher: 134.134.134.134:5
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:33333
Route Distinguisher: 201.201.201.201:2
*> [5]:[0]:[24]:[22.1.1.0]
                    201.201.201.201          0             0 201 i
                    RT:201:9999 ET:8 Rmac:c4:39:3a:fb:be:d9
Route Distinguisher: 201.201.201.201:3
*> [2]:[0]:[48]:[00:11:11:11:11:11]
                    201.201.201.201                       0 201 i
                    RT:201:9999 RT:201:22221 ET:8 Rmac:c4:39:3a:fb:be:d9
*> [2]:[0]:[48]:[00:11:11:11:11:11]:[32]:[21.1.1.1]
                    201.201.201.201                       0 201 i
                    RT:201:9999 RT:201:22221 ET:8 Rmac:c4:39:3a:fb:be:d9
*> [3]:[0]:[32]:[201.201.201.201]
                    201.201.201.201                       0 201 i
                    RT:201:22221 ET:8
Route Distinguisher: 201.201.201.201:4
*> [3]:[0]:[32]:[201.201.201.201]
                    201.201.201.201                       0 201 i
```

```
                    RT:201:22222 ET:8
```

run show bgp evpn route detail

The **run show bgp evpn route detail** command can be ued to display the detailed information of local BGP EVPN route entries in the routing table.

Command Syntax

run show bgp evpn route detail

Parameters

None.

Example

- Display the detailed information of local BGP EVPN routes in the routing table.

```
admin@SVNE2# run show bgp evpn route detail
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[00:00:00:00:00:00]
Paths: (0 available, no best path)
  Not advertised to any peer
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[00:00:00:00:00:00]
Paths: (0 available, no best path)
  Not advertised to any peer
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]
Paths: (0 available, no best path)
  Not advertised to any peer
Route Distinguisher: 10.226.14.24:7
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[32]:[192.168.20.24]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[32]:[192.168.20.24] VNI 10020/99
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
      Origin IGP, valid, external, best (First path received)
      Extended Community: RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
      Last update: Wed Nov  6 14:17:04 2024
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[::]
Paths: (0 available, no best path)
  Not advertised to any peer
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[2002:0:0:1::24]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[2002:0:0:1::24] VNI 10020/99
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
      Origin IGP, valid, external, best (First path received)
      Extended Community: RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
      Last update: Wed Nov  6 14:17:04 2024
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[fe80::529a:4c20:3e6:7e71]
Paths: (1 available, best #1)
```

```
 Advertised to non peer-group peers:
 rif-p17 rif-p19
 Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[fe80::529a:4c20:3e6:7e71] VNI 10020/99
 800 100
   10.226.14.201 from rif-p17 (39.39.39.39)
     Origin IGP, valid, external, best (First path received)
     Extended Community: RT:100:10020 ET:8
     Last update: Wed Nov  6 14:17:04 2024
--More--
```

run show bgp evpn route vni

The **run show bgp evpn route vni** command can be used to display BGP EVPN routes with specified VNI ID in the routing table.

Command Syntax

run show bgp evpn route vni <*vni***>**

Parameters

Parameter	Description
vni <*vni-id*>	Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.

Example

- Display BGP EVPN routes with VNI 10020 in the routing table.

```
admin@SVNE2# run show bgp evpn route vni 10020
BGP table version is 1416, local router ID is 10.226.14.208
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

   Network          Next Hop            Metric LocPrf Weight Path
*> [2]:[0]:[48]:[18:5a:58:37:55:e1]:[32]:[192.168.20.47]
                    10.226.14.254                       32768 i
                    ET:8 RT:400:10020 RT:400:99 Rmac:18:5a:58:37:55:e1
*> [2]:[0]:[48]:[18:5a:58:37:55:e1]:[128]:[2002:0:0:1::47]
                    10.226.14.254                       32768 i
                    ET:8 RT:400:10020 RT:400:99 Rmac:18:5a:58:37:55:e1
*> [2]:[0]:[48]:[18:5a:58:37:55:e1]:[128]:[fe80::1a5a:5810:137:55e1]
                    10.226.14.254                       32768 i
                    ET:8 RT:400:10020
*> [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[32]:[192.168.20.24]
                    10.226.14.201                           0 800 100 i
                    RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
*> [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[2002:0:0:1::24]
                    10.226.14.201                           0 800 100 i
                    RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
*> [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[fe80::529a:4c20:3e6:7e71]
                    10.226.14.201                           0 800 100 i
                    RT:100:10020 ET:8
*  [2]:[0]:[48]:[8c:ea:1b:a8:c5:41]
                    10.226.14.201                           0 800 200 i
                    RT:200:10020 ET:8
```

```
*> [2]:[0]:[48]:[8c:ea:1b:a8:c5:41]
                    10.226.14.201                          0 800 100 i
                    RT:100:10020 ET:8
*  [2]:[0]:[48]:[8c:ea:1b:a8:c5:41]:[32]:[192.168.20.135]
                    10.226.14.201                          0 800 100 i
                    RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
*> [2]:[0]:[48]:[8c:ea:1b:a8:c5:41]:[32]:[192.168.20.135]
                    10.226.14.201                          0 800 200 i
                    RT:200:99 RT:200:10020 ET:8 Rmac:90:3c:b3:4c:af:f9
*  [2]:[0]:[48]:[8c:ea:1b:a8:c5:41]:[128]:[fe80::8eea:1b10:3a8:c541]
                    10.226.14.201                          0 800 200 i
                    RT:200:10020 ET:8 ND:Router Flag
 --More--
```

run show bgp evpn route rd

The command **run show bgp evpn route rd** can be used to display BGP EVPN routes with specified route distinguisher in the routing table.

Command Syntax

run show bgp evpn route rd <*rd***>**

Parameters

Parameter	Description
rd <*rd***>**	Specifies the route distinguisher. The value follows the format RouterID:VNI-Index.

Example

- Display all BGP EVPN routes with route distinguisher 10.226.14.24:7.

```
admin@SVNE2# run show bgp evpn route rd 10.226.14.24:7
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[32]:[192.168.20.24]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[32]:[192.168.20.24] VNI 10020/99
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
      Origin IGP, valid, external, best (First path received)
      Extended Community: RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
      Last update: Wed Nov  6 14:17:05 2024
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[2002:0:0:1::24]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[2002:0:0:1::24] VNI 10020/99
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
      Origin IGP, valid, external, best (First path received)
      Extended Community: RT:100:99 RT:100:10020 ET:8 Rmac:50:9a:4c:e6:7e:71
      Last update: Wed Nov  6 14:17:05 2024
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[fe80::529a:4c20:3e6:7e71]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[50:9a:4c:e6:7e:71]:[128]:[fe80::529a:4c20:3e6:7e71] VNI 10020/99
```

```
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
      Origin IGP, valid, external, best (First path received)
      Extended Community: RT:100:10020 ET:8
      Last update: Wed Nov  6 14:17:05 2024
BGP routing table entry for 10.226.14.24:7:[2]:[0]:[48]:[8c:ea:1b:a8:c5:41]
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
  rif-p17 rif-p19
  Route [2]:[0]:[48]:[8c:ea:1b:a8:c5:41] VNI 10020
  800 100
    10.226.14.201 from rif-p17 (39.39.39.39)
 --More--
```

run show bgp evpn route type

The **run show bgp evpn route type** command displays BGP EVPN routes of specified type in the routing table.

Command Syntax

run show bgp evpn route type [**ead** | **es** | **macip** | **multicast** | **prefix**]

Parameters

Parameter	Description
type [**ead** | **es** | **macip** | **multicast** | **prefix**]	Specifies the EVPN type as **ead**(type1), **es**(type4), **macip**(type2), **multicast**(type3) or **prefix**(type5).

Example

- Display all BGP EVPN routes of type **multicast**(type3).

```
admin@SVNE2# run show bgp evpn route type multicast
BGP table version is 594, local router ID is 10.226.14.208
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[EthTag]:[ESI]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

   Network          Next Hop            Metric LocPrf Weight Path
                    Extended Community
Route Distinguisher: 10.226.14.24:7
*> [3]:[0]:[32]:[10.226.14.201]
                    10.226.14.201                          0 800 100 i
                    RT:100:10020 ET:8
Route Distinguisher: 10.226.14.24:8
*> [3]:[0]:[32]:[10.226.14.201]
                    10.226.14.201                          0 800 100 i
                    RT:100:10030 ET:8
Route Distinguisher: 10.226.14.48:3
*> [3]:[0]:[32]:[10.226.14.202]
                    10.226.14.202                          0 500 i
                    RT:500:10020 ET:8
Route Distinguisher: 10.226.14.48:4
*> [3]:[0]:[32]:[10.226.14.202]
                    10.226.14.202                          0 500 i
                    RT:500:10030 ET:8
Route Distinguisher: 10.226.14.208:3
*> [3]:[0]:[32]:[10.226.14.254]
                    10.226.14.254                     32768 i
                    ET:8 RT:400:10020
```

```
Route Distinguisher: 10.226.14.208:4
*> [3]:[0]:[32]:[10.226.14.254]
                    10.226.14.254                     32768 i
                    ET:8 RT:400:10030
Route Distinguisher: 17.17.17.17:3
*> [3]:[0]:[32]:[10.226.14.201]
                    10.226.14.201                         0 800 200 i
                    RT:200:10020 ET:8
Route Distinguisher: 17.17.17.17:4
*> [3]:[0]:[32]:[10.226.14.201]
                    10.226.14.201                         0 800 200 i
                    RT:200:10030 ET:8
```

PoE Configuration Commands

Power over Ethernet (PoE) is a convenient way to deliver electrical power to network devices. Rather than running power over a separate electrical circuit, with PoE electrical power is carried over Ethernet cables, meaning only one cable connection is required to the device. Enabling PoE requires administrators to become familiar with a series of PoE commands. This page provides links to 11 of those commands. Follow the links to learn how to set max power thresholds, set PoE detection type, enable or disable PoE on a port-by-port basis, set the type of power limit on specific ports (PoE interface threshold mode), display PoE power status and more.

- set poe interface max-power
- set poe interface detection-type
- set poe interface enable
- set poe interface mode
- set poe interface priority
- set poe interface threshold-mode
- set poe power management-mode
- set poe power mode
- set poe interface lldp-negotiation
- set poe power voltage
- set poe traceoptions flag all disable
- run show poe interface
- run show poe power
- set poe perpetual-power enable

set poe interface max-power

NOTE:
This command is not available for S5810-48TS-P, S5860-24XB-U, S3410-24TF-P, N32xx, S3410C-16TF-P, S3410C-16TMS-P and S3410C-8TMS-P series switches:

- On **N3248PXE-ON**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 99 watts.
- On **N3248P-ON**, all the RJ45 ports of the switch support PoE but not UPoE, the maximum output power of each port is 30 watts.
- On **N3224PX-ON**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 99 watts.
- On **N3224P-ON**, all the RJ45 ports of the switch support PoE but not UPoE, the maximum output power of each port is 30 watts.
- On **S5860-24XB-U**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 90 watts.
- On **S3410-24TF-P**, all the RJ45 ports of the switch support PoE, the maximum output power of each port is 30 watts.
- On **S3410C-8TMS-P**, only the first eight RJ45 ports of the switch support PoE, the maximum output power of each port is 30 watts.

The **set poe interface max-power** command configures maximum output power of all the ports or a specific port.

Command Syntax

set poe interface {<*interface-name*> | **all**} **max-power** <*integer*>

Parameter

Parameter	Description
interface {< *interface-name* > | **all**}	Specifies interface name. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that sets a same maximum output power on all RJ45 ports.

max-power <*integer***>**	Specifies maximum output power of a port. The value is an integer, the unit is watt.
	• On **AS4610-30P** and **AS4610-54P**,
	  ◦ Only the last 8 RJ45 ports of the switch, which are, ge-1/1/17 - ge-1/1/24 on AS4610-30P, ge-1/1/41 - ge-1/1/48 on AS4610-54P, support UPoE.
	  ◦ For UPoE ports the range is from 1W to 51W, for other ports the range is from 1W to 32W. The default value is 16W.
	• On **AS4630-54NPE**/**AS4630-54PE**, the first 48 RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power can be set up to 90 watts, the default value is 30 watts.
	• On **AS4625-54P**, the 48 x 1G RJ45 ports on the front panel support PoE. Port1~Port40 support supports IEEE802.3at/af, the maximum output power supported is up to 30 watts, Port41~Port48 support IEEE802.3bt standard, the maximum output power supported is up to 90 watts.
	• On **S5860-24MG-U**, the 24 x 10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power can be set up to 90 watts.
	• On **S5860-48XMG-U**, the first 48 x 10G RJ45 ports on the front panel support PoE, only the first 24 x 10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts. For other PoE ports, the maximum output power supported is 30 watts.
	• On **S3410-24TS-P**, the 24 x 1G RJ45 ports on the front panel support PoE. For these PoE ports, the maximum output power can be set up to 30 watts.
	• On **S3410C-8TMS-P**, the 2 x 5G and first 6 x 1G RJ45 ports on the front panel support PoE. For these PoE ports, the maximum output power can be set up to 30 watts.
	• On **S3410-48TS-P**, the 48 x 1G RJ45 ports on the front panel support PoE. For these PoE ports, the maximum output power can be set up to 30 watts.

Usage Guidelines

Maximum output power configured on a specific port has a higher priority than that of global configuration. For example,

```
admin@Xorplus# set poe interface all max-power 20
admin@Xorplus# set poe interface ge-1/1/7 max-power 25
```

The result of the above configuration is: the maximum output power on ge-1/1/7 port is 25W, other ports are 20W.

NOTE:

- To make the set of max-power take effect, user need to disable and re-enable PoE function of the interface by using the **set poe interface {**<*port-id*> | **all} enable <true | false>** command.
- The max-power value should be at least 20% greater than the consumed power of the interface. We can use the **run show poe interface** {<*port-id*> | **all**} command to find the consume power.
- PoE over LLDP power negotiation takes a precedence over the max-power configured on the switch. If PoE over LLDP power negotiation function is enabled, the power value provided by PICA8 switch uses power over LLDP negotiation rather than the power value configured on the switch interface.

Example

- Set the maximum output power of port ge-1/1/7 to 30W.

```
admin@Xorplus# set poe interface ge-1/1/7 max-power 30
admin@Xorplus# commit
```

set poe interface detection-type

This command is applied on AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U and S3410-24TS-P.

The **set poe interface detection-type** command configures PoE detection type of all the ports or a specific ethernet port.

Command Syntax

set poe interface {<*port-id*> | **all**} **detection-type** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same detection type on all ports.
detection-type <*value*>	Specifies PoE detection type, the value is an integer that ranges from 0 to 5. 0: NO detection. 1: Legacy capacitive detection only. 2: IEEE 802.3af 4-Point detection only. 3: IEEE 802.3af 4-Point followed by legacy. 4: IEEE 802.3af 2-Point(not support). 5: IEEE 802.3af 2-Point followed by legacy. The default value is 3.

Note:

Configuration on a specific port has a higher priority than that of global configuration.

Example

This example is to configure PoE detection-type 5 on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all detection-type 5
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 detection-type 5
admin@XorPlus# commit
```

set poe interface enable

The **set poe interface enable** command enables PoE function on all ports or on a specific port.

Command Syntax

set poe interface {<*port-id*> | **all**} **enable** <**true | false**>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies port ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that enable or disable PoE on all ports.
enable <**true | false**>	Enable or disable PoE function. • **true**: enable PoE function. • **false**: disable PoE function. By default, PoE function is disabled.

Note:

Configuration on a specific port has a higher priority than that of global configuration. For example, if a specific port enables PoE function but the global configuration disables PoE function, then PoE function of all ports is disabled except this specific port.

Example

• This example is to enable PoE on all the ports and ge-1/1/1.

```
admin@XorPlus# set poe interface all enable true
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 enable true
admin@XorPlus# commit
```

set poe interface mode

This command is applied on AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U, S3410-24TS-P and S3410-48TS-P.

The **set poe interface mode** command configures PoE pair mode on all the ports or a specific physical port.

Command Sytax

set poe interface {<*port-id*> | **all**} **mode** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same mode on all ports.
mode <*value*>	Specifies PoE pair mode, the value can be **signal** and **spare**. • **signal**: Pair type A, deliver power with data transmit wires. • **spare**: Pair type B, deliver power with spare wires. The default value is signal.

Note:

Configuration on a specific port has a higher priority than that of global configuration.

Example

This example is to configure pair mode spare on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all mode spare
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 mode spare
admin@XorPlus# commit
```

set poe interface priority

The **set poe interface priority** command configures PoE priority on all the ports or on a specific ethernet port.

Command Syntax

On AS4610-30P, AS4610-54P, AS4630-54PE, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U, S3410-24TF-P, S3410-24TS-P and S3410C-8TMS-P:

set poe interface {<*port-id*> | **all**} **priority** <**critical | high | medium | low**>

On other PoE supported switches:

set poe interface {<*port-id*> | **all**} **priority** <**critical | high | low**>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set all ports with a same PoE priority.
priority <**critical | high | medium | low**>	Specifies PoE priority. On AS4610-30P, AS4610-54P, AS4630-54PE, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U, S3410-24TF-P, S3410-24TS-P, S3410C-16TMS-P, S3410C-16TF-P and S3410C-8TMS-P: The value is **critical**, **high**, **medium** and **low**. The priority is: critical > high > medium > low. The default value is medium. On other PoE supported switches: The value is **critical**, **high** and **low**. The priority is: critical > high > low. The default value is low.

Usage Guidlines

Configuration on a specific port has a higher priority than that of global configuration. For example, if the global configuration of PoE priority is set to high, while PoE priority on a specific port is set to critical, then PoE priority on this specific port is critical, other ports are high.

If a port is set as higher priority and a situation arises where there is not sufficient power for all the PoE ports, the available power is directed to the higher priority port(s). If the switch needs to shut down powered devices because a power supply fails and there is insufficient power, low priority devices are shut before high priority powered devices. Thus, security cameras, emergency phones, and other high priority devices should be set to a high priority.

Example

This example is to configure priority critical on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all priority critical
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 priority critical
admin@XorPlus# commit
```

set poe interface threshold-mode

This command is applied on AS4610-30P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U, S3410-24TS-P and S3410-48TS-P.

The **set poe interface threshold-mode** configures PoE threshold-mode on all the ports or a specific physical port.

Command Syntax

set poe interface {<*port-id*> | **all**} **threshold-mode** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same threshold mode on all ports.
threshold-mode <*value*>	The value is an interger that ranges from 0 to 2. 0: None (max power 16.2W) (Default). 1: Class Based (allows the port to draw up to advertised class max). 2: User defined (User-defined max power value), configured through max power threshold configuration command below. This command configures the type of power limit on the specific port. For the class-based power threshold, the class max power values are as follows: Class 0: 16.2W Class 1: 4.2W Class 2: 7.4W Class 3: 15W Class 4: 30W Class 5: 45W Class 6: 60W Class 7: 75W Class 8: 90W

Example

• This example is to configure threshold-mode 2 (user defined) on all the ports and ge-1/1/1.

```
admin@XorPlus# set poe interface all threshold-mode 2
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 threshold-mode 2
admin@XorPlus# commit
```

set poe power management-mode

This command is not available for S5810-48TS-P, S5860-24XB-U, S3410-24TF-P,S3410C-16TMS-P, S3410C-16TF-P, S3410C-8TMS-P, N32xx and N22xx series switches.

The **set poe power management-mode** command configures PoE power management-mode on all the ports or on a specific ethernet port.

Command Syntax

set poe power management-mode <*value*>

Parameter

<*value*>*:* The value is an integer that ranges from 1 to 4. The default value is 1.

1	Static Power Management with Port Priority
2	Dynamic Power Management with Port Priority
3	Static Power Management without Port Priority
4	Dynamic Power Management without Port Priority

1:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power is greater than the maximum power threshold configured on the port, and total allocated power is below the guard band.
- When the available power is less than the maximum power threshold configured on the port and the port priority is lower than the priority of all powered ports the PoE controller does not allow power on the port.
- When the available power is less than the maximum power threshold configured on the port and the port priority is greater than the priority of powered ports, the PoE controller disconnects low priority ports and allows the higher priority port to power up.

2:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power from the power source is greater than the maximum power threshold configured on the port and the total allocated power is below the guard band.
- When available power is less than the maximum power threshold configured on the port and port priority is less than the port priority set on all powered ports, the PoE controller does not allow power on the port.
- When available power is less than the maximum power threshold configured or the port and the port priority is greater than the priority of currently powered ports, the PoE controller disconnects the low priority ports and allows the port to power up.
- When the total consumed power exceeds the configured power limit of power source, low priority ports are turned off.

3:

- When a PD is detected on a specific port,the PoE controller allows power on the port if available power is greater than the maximum power threshold configured on the port, and total allocated power is below the guard band.
- When the available power is less than the maximum power threshold configured on the port, the PoE controller does not allow power on this port since port priority is not taken into effect, lower priority ports are not disconnected to power higher priority ports.

4:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power from the power source is greater than the maximum power threshold configured on the port and the total allocated power is below the guard band.
- When the total consumed power exceeds the configured power limit of power source, the PoE controller starts powering down the ports beginning with the highest port number.

Example

This example is to configure power management-mode to 1:

```
admin@XorPlus# set poe power management-mode 1
admin@XorPlus# commit
```

set poe power mode

The **set poe power mode** command configures PoE power mode to aggressive or redundant.

Command Syntax

set poe power mode <**aggressive** | **redundant**>

Parameter

Parameter	Description
mode <**aggressive** | **redundant**>	For details about the maximum power values supported by each PoE supported platform for the two PoE power modes, see Table 1.

Usage Guidelines

The maximum power value on S3410C-16TMS-P does not distinguish between high and low voltages, and the POE supports a maximum power of 800 watts.

The maximum power value on S3410C-16TF-P does not distinguish between high and low voltages, and the POE supports a maximum power of 800 watts.

The maximum power value on S3410-24TF-P does not distinguish between high and low voltages, and the PoE power mode is only redundant with the maximum power value 800 Watts.

The maximum power value on S3410-24TS-P and S3410-48TS-P does not distinguish between high and low voltages, the maximum power value is 740 Watts in aggressive mode and 370 Watts in redundant mode**.**

The maximum power value on S5810-48TS-P, S5860-24XB-U and S3410C-8TMS-P does not distinguish between high and low voltages, the maximum power value is 1500 Watts in aggressive mode and 750 Watts in redundant mode**.**

The maximum power value on S5860-24MG-U does not distinguish between high and low voltages, the maximum power value is 648 Watts in aggressive mode and 324 Watts in redundant mode.

The maximum power value on S5860-48XMG-U does not distinguish between high and low voltages, the maximum power value is 765 Watts in aggressive mode and 382.5 Watts in redundant mode.

Table 1. The maximum power values supported by each PoE supported platform

Power Mode	High Voltage（Voltage>120V）		Low Voltage（Voltage<120V）	
	Aggressive (Watts)	Redundant (Watts)	Aggressive (Watts)	Redundant (Watts)
N3248PXE-ON	2496	1056	1261	406
N3248P-ON	1758	813	1568	713
N3208PX-ON	493	193	493	193
N3224PX-ON	2700	1260	1465	610
N3224P-ON	1771	826	1581	726
AS4610_54P	1500	750	800	400
AS4610_30P	1500	750	800	400
AS4630-54PE	1800	900	1000	500
AS4630-54NPE	1800	900	1000	500
N2248PX-ON	2714	1274	1479	624
N2224PX-ON	1757	812	1567	712
N3224P-ON	1771	826	1581	726
AS4625-54P	2025	945	1665	765

Example

- Configure power mode to aggressive.

```
admin@XorPlus# set poe power mode aggressive
admin@XorPlus# commit
```

set poe interface lldp-negotiation

> This command is not available for S5810-48TS-P, S3410-24TF-P,S3410C-16TMS-P, S3410C-16TF-P, S3410C-8TMS-P and S5860-24XB-U.

The **set poe interface lldp-negotiation** command is used to enable or disable PoE over LLDP power negotiation function on all ports or on a specific port.

Command Syntax

set poe interface <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**>

Parameter

Parameter	Description
interface {**all** | *interface-name*}	Specifies an interface name. The value could be **all** or a specific interface name, **all** indicates a global configuration that enables or disables the PoE over LLDP power negotiation function on all ports.
lldp-negotiation {**true** | **false**}	Enables or disables the PoE over LLDP power negotiation function. The value is **true** or **false**. • **true**: enables the PoE over LLDP power negotiation function. • **false**: disables the PoE over LLDP power negotiation function. The default value is **true**.

Usage Guidelines

PoE over LLDP power negotiation function allows the switch to assign the power priority and power value provided by the powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority and power value configured on the switch interface.

By default, PoE over LLDP power negotiation function is globally enabled for all the interfaces. It can be configured globally and per-interface, and the per-interface configuration takes a precedence over the global configuration.

When an expansion module is connected to the IP phone, in order to provide the required power to the expansion module, user should perform the following two operations to re-negotiate the PoE power supply.

1). Enable the PoE over LLDP power negotiation function on the interface by using **set poe interface** <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**> command.

2). Disable and re-enable PoE function of the interface by using **set poe interface {**<*port-id*> | **all} enable <true | false>** command.

> **NOTE:**
> - Enable LLDP function and PoE function before using PoE over LLDP power negotiation.
> - Enable PoE over LLDP power negotiation function when there is an expansion module connected to the IP phone.

Example

- Disable the PoE over LLDP power negotiation function on interface Ge-1/1/1.

```
admin@Xorplus# set poe interface ge-1/1/1 lldp-negotiation false
admin@Xorplus# commit
```

- Enable the PoE over LLDP power negotiation function on interface Ge-1/1/1.

```
admin@Xorplus# set poe interface ge-1/1/1 lldp-negotiation true
admin@Xorplus# commit
```

set poe power voltage

> **NOTE:**
> This command is applied on AS4630-54NPE and AS4630-54PE.

The **set poe power voltage** command configures PoE power voltage on AS4630-54NPE and AS4630-54PE platforms.

The **delete poe power voltage** command deletes the configuration.

Command Syntax

set poe power voltage [**110v | 220v**]

Parameters

Parameter	Description
voltage [**110v** | **220v**]	Specifies the voltage value. The value could be **110v** or **220v**.The default value is **110v**.

Usage Guidelines

On AS4630-54NPE and AS4630-54PE, PICOS cannot read out the voltage. Users can use command **set poe power voltage** [**110v | 220v**] to set PoE power voltage. With different voltage, 110V-120V at low-line or 220V-240V at high-line, each PSDU will give 1000W or 1200W respectively. Accordingly, the switch will allocate different power to PoE with regarding to low-line or high-line. By accounting for the PoE guard band (10%), the PoE available powers are illustrated by below table.

With two PSUs powered on:

Voltage / Power Mode	Low-line (110V)	High-line (220V)
redundant	700W x 90% = 630W	900W x 90% = 810W
aggressive	1700W x 90% = 1530W	2100W x 90% = 1890W

With one PSU powered on:

Voltage / Power Mode	Low-line (110V)	High-line (220V)
redundant	700W x 90% = 630W	900W x 90% = 810W
aggressive	700W x 90% = 630W	900W x 90% = 810W

Example

- Configure PoE power voltage on AS4630-54NPE or AS4630-54PE.

```
admin@Xorplus# set poe power voltage 110v
admin@Xorplus# commit
```

When PoE power mode is *redundant*, the result of “run show poe power” shows as below:

```
Total power allocated  RealTime consumption   Power available  Power Mode      PSU1 Status           PSU2 Status
---------------------  --------------------   ---------------  ----------      -----------           ------------
0.00W                  0.00W                  630.00W          redundant       Powered on            Powered on
```

When PoE power mode is *aggressive*, the result of “run show poe power” shows as below:

```
root@PICOS# run show poe power
Total power allocated  RealTime consumption   Power available  Power Mode      PSU1 Status           PSU2 Status
---------------------  --------------------   ---------------  ----------      -----------           ------------
0.00W                  0.00W                  1530.00W         aggressive      Powered on            Powered on
```

set poe traceoptions flag all disable

The **set poe traceoptions flag all disable** command can be used to enable or disable PoE debugging for tracing all PoE operations.

The **delete poe traceoptions flag all disable** command deletes the configuration.

Command Syntax

set poe traceoptions flag all disable <**true | false**>

delete poe traceoptions flag all disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable PoE debugging for tracing all PoE operations. The value could be **true** or **false**. • **true**: Disable PoE debugging for tracing all PoE operations. • **false**: Enable PoE debugging for tracing all PoE operations. By default, the PoE debugging for tracing all PoE operations is disabled.

Example

- Enable PoE debugging for tracing all PoE operations.

```
admin@PICOS# set poe traceoptions flag all disable false
admin@PICOS# commit

```

run show poe interface

The **run show poe interface** command displays the PoE status of all the ports or on a specific ethernet port.

Command Sytax

run show poe interface {*<port-id>* | **all**}

Parameter

Parameter	Description
interface {*<port-id>* | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates to display PoE status of all the ports.

Example

• This example is to show poe interface of ge-1/1/1:

```
admin@XorPlus# run show poe interface ge-1/1/1
Port       Status    Consume   Reserved   Pair  PD_Type  PD-Class   Detection_Type
------------------------------------------------------------------------------
ge-1/1/1   Searching   2.80W    16.20W     A    IEEE          2     IEEE 802.3af 4-Point
```

• This example is to show poe interface of all the ports:

```
admin@XorPlus# run show poe interface all
Port       Status    Consume  Reserved Pair  PD_Type   PD-Class   Detection_Type
------------------------------------------------------------------------------
ge-1/1/1   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/2   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/3   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/4   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/5   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/6   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/7   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/8   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/9   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/10  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/11  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/12  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/13  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/14  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/15  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/16  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/17  Searching  0.00W  0.00W      A    None    4   IEEE 802.3af 4-Point
ge-1/1/18  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/19  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/20  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/21  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/22  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/23  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/24  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/25  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/26  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/27  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/28  Delivering 1.10W  16.2W      A    IEEE    2    IEEE 802.3af 4-Point
ge-1/1/29  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/30  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/31  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/32  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/33  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/34  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/35  Delivering 1.30W  16.2W      A    IEEE    2    IEEE 802.3af 4-Point
ge-1/1/36  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/37  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
```

```
ge-1/1/38  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/39  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/40  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/41  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/42  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/43  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/44  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/45  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/46  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/47  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/48  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
```

Table 1 Description of the run show poe interface all command output of AS4610-30P, AS4610-54P

Item	Description
Port	Port ID.
Status	Indicates that PoE function status, the value could be **Disabled**, **Searching**, **Delivering**, **Test**, **Requesting** and **Fault**.
Consume	Indicates the power consumption of port.

Reserved	Indicates the power allocated.
	• When PoE over LLDP power negotiation is enabled, it shows the negotiated power.
	• When PoE over LLDP power negotiation is disabled,
	  • If mangement mode is dynamic, the allocated power is same to the consumption power on AS4610-30P, AS4610-54P, AS4630-54PE and AS4630-54NPE
	  • If mangement mode is static, the allocated power is the configured max-power on AS4610-30P, AS4610-54P, AS4630-54PE and AS4630-54NPE.

Pair	Indicates PoE pair mode. **A**: signal, deliver power with data transmit cable. **B**: spare, deliver power with spare cable.
PD_Type	Indicates powered device type, the value could be **None**, **IEEE**, **Pre-Standard** and **Extended**.
PD_Class	Indicates the PD class, the value could be **1**, **2**, **3**, **4**.
Detection_Type	Indicates PoE detection type, the value could be: **no detection** **Legacy Capacitive Detection only** **IEEE 802.3af 4-Point Detection only** **IEEE 802.3af 4-Point followed by Legacy** **IEEE 802.3af 2-Point Detection** **IEEE 802.3af 2-Point followed by Legacy**

run show poe power

The **run show poe power** command displays the PoE power status.

Note:

On AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P and AS4630-54NPE,

- If Power Management mode is dynamic, total power allocated is about the same value as realtime consumption.
- But if Power Management mode is static, total power allocated is usually larger than realtime consumption.

On other PoE supported switches, regardless of whether Power Management mode is dynamic or static, the total power allocated is about the same value as realtime consumption.

Example

- Displays the PoE power status.

On AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24XB-U, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U, S3410C-8TMS-P and S3410-48TS-P:

```
admin@XorPlus# run show poe power
Total power allocated          RealTime consumption     Power available   Power Mode    PSU1 Status    PSU2 Status
-------------------------------------------------------------------------------------------------------------------
2.20W                          2.20W                     675.00W         redundant       Powered on          Prese
```

On other PoE supported switches:

```
root@Xorplus# run show poe power
Consumption Power  Calculated Power  Available Power   PSU1 Status           PSU2 Status
-------------------------------------------------------------------------------------------------------------
0W                 0W               950W              Not present           Powered on
```

Table 1 Description of the run show poe power command output

Item	Description
Total power allocated	Total allocated max power for all ports.
RealTime consumption	The actual consumption power of all ports.
Power available	The max limit power value of PSE.
Consumption Power	The actual power consumed by all ports.
Calculated Power	The sum of all ports power, allocated as defined by IEEE standard 802.3af-2003, or actually consumed.
Available Power	The max limit power value of PSE.
Power Mode	Redundant or aggressive based on set.
PSU1 Status	Status of PSU1.
PSU2 Status	Status of PSU2.

set poe perpetual-power enable

The **set poe perpetual-power enable** command is used to enable or disable perpetual PoE on the switch.

The **delete poe perpetual-power enable** command is used to restore the default configuration.

Command Syntax

set poe perpetual-power enable <**true** | **false**>

delete poe perpetual-power enable

Parameter

Parameter	Description
enable <**true** | **false**>	Enables or disables the perpetual PoE function. The value is **true** or **false**. • **true**: enables the perpetual PoE function. • **false**: disables the perpetual PoE function. By default, perpetual PoE is disabled.

Usage Guidelines

Enabling Perpetual PoE ensures that connected PoE devices continue to receive power even when the switch undergoes a reboot. This is particularly useful for devices that require constant power, such as security cameras, VoIP phones, and wireless access points, preventing downtime and ensuring continuous operation.

When configuring perpetual PoE, consider the following points:

- Only S5860-24XB-U switch supports perpetual PoE.
- Perpetual PoE supports maintaining uninterrupted power during a system reboot in the following scenarios.
  a. Execute the command **request system reboot** in L2/L3 CLI operating mode.

```
admin@PICOS> request system reboot
```

  b. Execute the **reboot** command in the Linux shell.

```
admin@PICOS:~$ sudo reboot
```

  c. Reboot during the upgrade process.

  d. For **nos-rollback** operation, if the version being rolled back to does not have Perpetual PoE configured, Perpetual PoE will not maintain uninterrupted power during the reboot in the NOS rollback process.

- Before restarting the S5860-24XB-U device, you need to save the configuration by executing **copy running-config startup-config** in L2/L3 CLI operating mode.
- Perpetual PoE will not maintain uninterrupted power in the following situations:

  a. Power failure or power cycling.

  b. PoE controller firmware update.

Example

- Enable the perpetual PoE function.

```
admin@Xorplus# set poe perpetual-power enable true
admin@Xorplus# commit
```

VRRP Commands

- set protocols vrrp interface vrid
- set protocols vrrp interface vrid disable
- set protocols vrrp interface vrid version
- set protocols vrrp interface vrid ip
- set protocols vrrp interface vrid priority
- set protocols vrrp interface vrid interval
- set protocols vrrp interface vrid preempt enable
- set protocols vrrp interface vrid load-balance disable
- set protocols vrrp interface vrid load-balance virtual-mac time-interval
- set protocols vrrp interface vrid accept disable
- set protocols vrrp interface vrid authentication type
- set protocols vrrp interface vrid simple-key
- set protocols vrrp interface vrid md5-key
- run show vrrp
- set protocols vrrp interface vrid ipv6-nd adv-interval-option
- set protocols vrrp interface vrid ipv6-nd home-agent-config-flag
- set protocols vrrp interface vrid ipv6-nd home-agent-lifetime
- set protocols vrrp interface vrid ipv6-nd home-agent-preference
- set protocols vrrp interface vrid ipv6-nd managed-config-flag
- set protocols vrrp interface vrid ipv6-nd mtu
- set protocols vrrp interface vrid ipv6-nd other-config-flag
- set protocols vrrp interface vrid ipv6-nd prefix off-link
- set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix router-address
- set protocols vrrp interface vrid ipv6-nd ra-fast-retrans
- set protocols vrrp interface vrid ipv6-nd ra-interval
- set protocols vrrp interface vrid ipv6-nd ra-lifetime
- set protocols vrrp interface vrid ipv6-nd reachable-time
- set protocols vrrp interface vrid ipv6-nd router-preference
- set protocols vrrp interface vrid ipv6-nd suppress-ra

set protocols vrrp interface vrid

The **set protocols vrrp interface vrid** command creates a VRRP group.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Usage Guidelines

When configuring VRID, pay attention to the following points:

- A VRID identifies the devices of the same VRRP group. Two devices in a VRRP group must be configured with the same VRID.
- It is recommended that VRRP groups on different L3 interfaces of a device should be configured with different VRIDs.
- One chassis switch supports a maximum of 128 VRRP groups. Please set the number of VRRP group based on device performance.

Example

- Create a VRRP group on vlan100 with VRID 2.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2
admin@Xorplus# commit
```

set protocols vrrp interface vrid disable

The **set protocols vrrp interface vrid disable** command is used to enable or disable the VRRP function.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
disable <**true	false**>	Enables or disables the VRRP function. The value is **true** or **false**. • **true**: disables the VRRP function. • **false**: enables the VRRP function. By default, VRRP function is enabled.

Example

- Disable the VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable true
admin@Xorplus# commit
```

- Enable the VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid version

The **set protocols vrrp interface vrid version** command assigns the VRRP version on the VRRP-enabled device.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **version** <**2** | **3**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
version <**2** | **3**>	Specifies the VRRP version. The value could be **2** or **3**, indicating VRRPv2 or VRRPv3. By default, the system uses VRRPv2.

Usage Guidelines

VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses. That is,

- A VRRPv2 group can send and receive only VRRPv2 Advertisement packets. The VRRPv2 group discards the received VRRPv3 Advertisement packets.
- A VRRPv3 group can send and receive both VRRPv2 and VRRPv3 Advertisement packets.

> **NOTE:**
>
> - As VRRPv2 and VRRPv3 interoperation is not supported, VRRP version must be the same on both devices of a VRRP group. If the VRRP versions on the switches in the VRRP group are different, which may result in abnormal VRRP operation.
> - When upgrading, we recommend that PICOS versions of the VRRP group devices be upgraded to PICOS 2.11.10 or later versions at the same time, as PICOS supports VRRPv3 from PICOS 2.11.10.

Example

- Assign the VRRP version.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 version 3
admin@Xorplus# commit
```

set protocols vrrp interface vrid ip

The **set protocols vrrp interface vrid ip** command assigns a virtual IP address to the VRRP group.

NOTE:

This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ip** <*ip-address*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ip <*ip-address*>	Specifies the virtual IPvX address of a VRRP group. The value could be an IPv4 address or an IPv6 address. Type the IPvX address without subnet mask as the mask value is the same as the Layer 3 interface.

Usage Guidelines

If users on a network have the same reliability requirements, configure multiple virtual IPvX addresses for a VRRP group. By doing this, one virtual IP address can serve one separate user group.

One VRRP group supports a maximum of 254 virtual IPv4 addresses, and 64 virtual IPv6 addresses.

Follow the rules below when configuring the virtual IPv4 / IPv6 address:

- For IPv4, the virtual IPv4 of the VRRP group and the IPv4 address of the interface should be configured in the same network segment to ensure that the VRRP group can work normally.
- For IPv6, the global virtual IPv6 address of the VRRPv3 group and the global IPv6 address of the interface should be configured in the same network segment to ensure that the VRRPv3 group can work normally.
- The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is the same as the virtual IP address is called an "IP address owner".
- The virtual IPv4 address of the VRRP group cannot be all zeros, broadcast address (255.255.255.255), network address or network broadcast address of the segment where the virtual IP address resides, loopback address, non-A / B / C address or any other illegal IP Address (e.g., 0.0.0.1).
- In the same VRRP group, IPv4 and IPv6 cannot be mixed. That is, the configured virtual IP addresses in the same VRRP group could either be virtual IPv4 addresses or virtual IPv6 addresses.
- For IPv6, configure at least one link-local IPv6 address in a VRRPv3 group which will be used as gateway address for the hosts, the format is FE80::/10.
- Virtual IP address list on both devices of VRRP group must be the same.
- Configure one or more global virtual IPv6 addresses, for the purpose of configuring global addresses via stateless address autoconfiguration of the downstream host (refer to RFC2462 IPv6 Stateless Address Autoconfiguration).

The gateway address of the downstream host should be configured as the virtual IPvX address of the VRRP virtual router device. For IPv6, the gateway address should be the virtual link-local address.

Example

- Assigns a virtual IP address to the VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ip 192.168.1.5
admin@Xorplus# commit
```

set protocols vrrp interface vrid priority

The **set protocols vrrp interface vrid priority** command sets the priority of the device in a VRRP group.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **priority** <*priority-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
priority <*priority-value*>	Specifies the priority of the device in a VRRP group. The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority. The default value is 100.

Usage Guidelines

VRRP determines the device role in the VRRP group based on device priority and L3 interface by exchanging VRRP advertisement packets. The device with a higher priority is more likely to become the master. If two devices have the same priority, the device with a larger interface IP address becomes the master.

The IP address owner's running priority is always 255, and no user configuration is required; the IP address owner always works in preemptive mode, regardless of whether the preemption function is enabled. If the VRRP device is the IP address owner, it will switch to the master state immediately after receiving the interface Up message.

For the backup device, if it has a higher priority than the master, the working mode of the backup (preemptive or non-preemptive) determines whether the master is re-selected.

- Preemptive mode: If the priority of the backup router is higher than the priority of the current master router, the backup router automatically becomes the master router.
- Non-preemptive mode: As long as the master router is working properly, the backup router with a higher priority cannot become the master router.

Example

- Set the priority of the switch in VRRP group 2 to 150 on the VLAN interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 priority 150
admin@Xorplus# commit
```

set protocols vrrp interface vrid interval

The **set protocols vrrp interface vrid interval** command sets the interval at which the VRRP device sends VRRP advertisement packets.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **interval** <*interval-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
interval <*interval-value*>	Specifies the interval at which the VRRP device sends VRRP advertisement packets. The value is an integer, in seconds. For VRRPv2, the value ranges from 1 to 255. For VRRPv3, the value ranges from 1 to 40. The default value is 4 seconds for both VRRPv2 and VRRPv3.

Usage Guidelines

If a larger interval is used, a backup device in the same VRRP group will not be able to detect the fault on the master in a timely fashion and can potentially cause packet loss. If a smaller interval is used, system resources are occupied. It is therefore recommended to set the interval based on actual network performance.

> **NOTE:**
>
> The configurations of the interval of sending VRRP advertisement packets on both devices of VRRP group must be the same.

Example

- Set the interval of sending VRRP advertisement to 5 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 interval 5
admin@Xorplus# commit
```

set protocols vrrp interface vrid preempt enable

The **set protocols vrrp interface vrid preempt enable** command configures the preemptive mode of the device in a VRRP group.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **preempt enable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
preempt enable <true | false>	Enables or disables the preemptive mode of the device. The value could be **true** or **false**. • **true**: enables the preemptive mode. Device in preemptive mode can preempt other nodes to be master if it has a higher priority. • **false**: disables the preemptive mode. Device in non-preemptive mode cannot preempt other nodes to be master even if it has the highest priority. By default, preemptive mode is enabled.

Usage Guidelines

To enable the device with higher priority in a VRRP group to be the master, set the preemptive mode on the device.

For the backup device, if it has a higher priority than the master, the working mode of the backup (preemptive or non-preemptive) determines whether the master is re-selected.

- Preemptive mode: If the priority of the backup router is higher than the priority of the current master router, the backup router automatically becomes the master router.
- Non-preemptive mode: As long as the master router is working properly, the backup router with a higher priority cannot become the master router.

By default, the preemptive mode is enabled, therefore, the device with a high priority is the master of the VRRP group.

> **NOTE:**
>
> The IP address owner always works in preemptive mode, regardless of whether the preemption function is enabled or not.

Example

- Enable the preemptive mode of the device in a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 preempt enable true
admin@Xorplus# commit
```

set protocols vrrp interface vrid load-balance disable

The **set protocols vrrp interface vrid load-balance disable** command is used to enable or disable the Active-Active VRRP function.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
disable <**true	false**>	Enables or disables the Active-Active VRRP function. The value is **true** or **false**. • **true**: disables the Active-Active VRRP function. • **false**: enables the Active-Active VRRP function. By default, Active-Active VRRP function is disabled.

Usage Guidelines

In the Standard VRRP protocol mode, only the Virtual Master Router can forward packets whereas the Virtual Backup Routers cannot forward packets. By adding a new working mechanism based on the VRRP standard protocol mode, Active-Active VRRP mode provides load balancing between the master and backup switches in the VRRP group, both of which are active, thus avoiding the situation where the backup switches are always idle in the Standard VRRP protocol mode. This greatly improves efficiency of network resources.

NOTE:

- To make the Active-Active VRRP function take effect, enable VRRP function by using set protocols vrrp interface vrid disable command.
- The Active-Active VRRP mode must be enabled or disabled on both devices of VRRP group.

Example

- Disable the Active-Active VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance disable true
admin@Xorplus# commit
```

- Enable the Active-Active VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid load-balance virtual-mac time-interval

The **set protocols vrrp interface vrid load-balance virtual-mac time-interval** command sets the interval at which the VRRP device sends virtual MAC update packets.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance virtual-mac time-interval** <*interval-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
time-interval <*interval-value*>	Specifies the interval at which the VRRP device sends virtual MAC update packets. The value is an integer, in seconds, the value ranges from 60 to14400. The default value 120s.

Usage Guidelines

To notify the downstream device of the virtual MAC, the master and backup devices send periodic virtual MAC update messages. The virtual MAC address in Active-Active VRRP mode is used in the Ethernet header of virtual MAC update packet as the source MAC address. The connected network devices of the VRRP group refresh their MAC entries in time in order to forward packets.

Example

- Set the interval of sending virtual MAC update packets to 80 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance virtual-mac time-interval 80
admin@Xorplus# commit
```

set protocols vrrp interface vrid accept disable

The **set protocols vrrp interface vrid accept disable** command is used to enable or disable the Accept Mode of the device in a VRRP group.

NOTE:

As Accept Mode is only supported in VRRPv3, this command applies to only VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **accept disable** <true | false>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
accept disable <true | false>	Enables or disables Accept Mode. The value could be **true** or **false**. • **true**: disables Accept Mode. • **false**: enables Accept Mode. By default, Accept Mode is disabled.

Usage Guidelines

VRRPv3 supports Accept Mode which controls whether a virtual router in Master state will accept packets addressed to the virtual IPvX address of a VRRP group if it is not the IP address owner (the IP address owner is the router that has the interface whose actual IP address is used as the virtual router's IP address).

By default, the Accept Mode is disabled, if the master is not the IP address owner, it only accepts the ARP requests/ARP replies or NS/NA messages addressed to the virtual IP, any other messages whose destination IP is the virtual IP are not accepted. But when accept mode is enabled, it can accept all packets whose destination IP is a virtual IP.

Deployments that rely on, for example, pinging the address owner's IPvX address may choose to configure Accept Mode to True.

NOTE:

- Accept Mode is only supported in VRRPv3 while VRRPv2 does NOT support. In VRRPv2, the master switch always accepts packets addressed to the virtual IPvX address.
- When Accept Mode is disabled, PICOS can still accept and process IPv6 Neighbor Solicitations / Neighbor Advertisements packets and ARP Request / ARP Reply packets.
- If the master is the IP address owner, it accepts all the packets addressed to the IPvX address(es) associated with the virtual router even though Accept Mode is disabled.

Example

- Enable the accept mode of the device in VRRP group 2.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 accept disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid authentication type

The **set protocols vrrp interface vrid authentication type** command configures an authentication mode for a VRRP group.

> **NOTE:**
>
> VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication type** <**none** | **md5** | **simple**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
authentication type <none | md5 | simple>	Specifies the authentication mode. The value could be **none**, **md5** or **simple**. • **none**: Indicates no authentication. • **md5**: Indicates MD5 authentication. • **simple**: Indicates simple authentication. By default, there's no authentication.

Usage Guidelines

NOTE:

- Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.
- If the VRRP authentication fails, the system prints the warning level log.

Example

- Enable MD5 authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 authentication type md5
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 md5-key picos123
admin@Xorplus# commit
```

set protocols vrrp interface vrid simple-key

The **set protocols vrrp interface vrid authentication simple-key** command configures the authentication key in simple authentication mode for a VRRP group.

NOTE:

VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication simple-key** <*simple-key*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
authentication simple-key <*simple-key*>	Specifies the authentication key in simple authentication mode. The value is a string of 1 to 8 case-sensitive characters without spaces.

Usage Guidelines

NOTE:

Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

- Configure the authentication key in simple authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 authentication simple-key picos123
admin@Xorplus# commit
```

set protocols vrrp interface vrid md5-key

The **set protocols vrrp interface vrid md5-key** command configures the authentication key in MD5 authentication mode for a VRRP group.

> **NOTE:**
>
> VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **md5-key** <*md5-key*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
md5-key <*md5-key*>	Specifies the authentication key in MD5 authentication mode. The value is a string of 1 to 16 case-sensitive characters without spaces.

Usage Guidelines

> **NOTE:**
>
> Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

- Configure the authentication key in MD5 authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 md5-key picos123
admin@Xorplus# commit
```

run show vrrp

The **run show vrrp** command displays the configuration information of VRRP group.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

run show vrrp *<interface-name>*

Parameter

Parameter	Description
<interface-name>	Optional. Specifies the Layer 3 interface name of VRRP device. The value is a string.

Example

- Run **run show vrrp** command to view the configuration information of VRRP group.

```
admin@XorPlus# run show vrrp vlan100
Interface: vlan100
VRID: 1
Version:                    3
Accept:  disable
Load-balance: enable
State: Master
Master IP: 192.168.1.1
Virtual MAC: 00:00:5e:00:01:01
Preempt: enable
Adver Interval: 4
Priority: 250
Virtual IP: 192.168.1.5
Auth-type:                  simple
Auth-key:                   123456
```

set protocols vrrp interface vrid ipv6-nd adv-interval-option

The **set protocols vrrp interface vrid ipv6-nd adv-interval-option** command includes an Advertisement Interval option which indicates to hosts the maximum time, in milliseconds, between successive unsolicited Router Advertisements for a VRRP group. Default: not set.

The **delete protocols vrrp interface vrid ipv6-nd adv-interval-option** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd adv-interval-option**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure to include an Advertisement Interval option between successive unsolicited Router Advertisements for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd adv-interval-option
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-config-flag

The **set protocols vrrp interface vrid ipv6-nd home-agent-config-flag** command sets flag in IPv6 router advertisements which indicates to hosts that the router acts as a Home Agent and includes a Home Agent Option. Default: not set.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-config-flag** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-config-flag**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure to set flag in IPv6 router advertisements which indicates to hosts that the router acts as a Home Agent and includes a Home Agent Option.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-config-flag
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-lifetime

The **set protocols vrrp interface vrid ipv6-nd home-agent-lifetime** command sets the value to be placed in Home Agent Option, when Home Agent config flag is set, which indicates to hosts Home Agent Lifetime.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-lifetime** <*home-agent-lifetime*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
home-agent-lifetime <*home-agent-lifetime*>	Specifies the lifetime of the home agent. The value is an integer, in seconds, that ranges from 0 to 65520. The default value of 0 means to place the current Router Lifetime value.

Example

- Configure the lifetime of the home agent to 120 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-lifetime 120
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-preference

The **set protocols vrrp interface vrid ipv6-nd home-agent-preference** command sets the value to be placed in Home Agent Option, when Home Agent config flag is set, which indicates to hosts Home Agent preference.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-preference** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-preference** <*home-agent-preference*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
home-agent-preference <*home-agent-preference*>	Specifies the preference of the home agent. The value is an integer, that ranges from 0 to 65535. The default value of 0 stands for the lowest preference possible. Default: 0.

Example

- Configure the preference of the home agent to 100.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-preference 100
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd managed-config-flag

The **set protocols vrrp interface vrid ipv6-nd managed-config-flag** command controls flag setting in RAs the router transmits on the current interface. Enable the flag to indicate that hosts can obtain IP address through DHCPv6. The flag is disabled by default.

The **delete protocols vrrp interface vrid ipv6-nd managed-config-flag** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd managed-config-flag**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure the flag in IPv6 router advertisements which indicates to hosts that they should use managed (stateful) protocol for addresses autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd managed-config-flag
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd mtu

The **set protocols vrrp interface vrid ipv6-nd mtu** command configures the MTU size to be sent in the RA messages.

The **delete protocols vrrp interface vrid ipv6-nd mtu** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd mtu** <*mtu-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
mtu <*mtu-value*>	Specifies the MTU size. Range: 1-65535 bytes.

Example

- Configure the MTU size to 1500 bytes.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd mtu 1500
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix off-link

The **set protocols vrrp interface vrid ipv6-nd prefix off-link** command configures that advertisement makes no statement about on-link or off-link properties of the prefix. Default: not set, i.e. this prefix can be used for on-link determination.

The **delete protocols vrrp interface vrid ipv6-nd prefix off-link** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **off-link [no-autoconfig]**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
no-autoconfig	Optional. Specifies do not use prefix for autoconfiguration. Default: not set, i.e. prefix can be used for autoconfiguration.

Example

- Configure that advertisement makes no statement about on-link or off-link properties of the prefix.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 off-link
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime

The **set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime** command configures the length of time in seconds during what the prefix is valid for the purpose of onlink determination.

The **delete protocols vrrp interface vrid ipv6-nd prefix valid-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **valid-lifetime {**<*LIFETIME-VALUE*>**|infinite}**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
valid-lifetime {<*LIFETIME-VALUE*>**|infinite}**	Specifies the length of time in seconds during what the prefix is valid for the purpose of onlink determination. Value **infinite** represents infinity (i.e. a value of all one bits (0xffffffff)). Range: (0-4294967295) Default: 2592000

Example

- Configure the length of time in seconds during what the prefix is valid for the purpose of onlink determination.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 valid-lifetime 2592000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime

The **set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime** command configures the length of time in seconds during what addresses generated from the prefix remain preferred.

The **delete protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **preferred-lifetime {**<*LIFETIME-VALUE*>**|infinite}**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
preferred-lifetime {<*LIFETIME-VALUE*>**|infinite}**	Specifies the length of time in seconds during what addresses generated from the prefix remain preferred. Value infinite represents infinity. Range: (0-4294967295) Default: 604800.

Example

- Configure the length of time in seconds during what addresses generated from the prefix remain preferred. Value infinite represents infinity.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 preferred-lifetime 604800
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix router-address

The **set protocols vrrp interface vrid ipv6-nd prefix router-address** command configures the router-address, indicating to hosts on the local link that the specified prefix contains a complete IP address by setting R flag. Default: not set, i.e. hosts do not assume a complete IP address is placed.

The **delete protocols vrrp interface vrid ipv6-nd prefix router-address** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **router-address**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.

Example

- Configure the router-address, indicating to hosts on the local link that the specified prefix contains a complete IP address by setting R flag.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 router-address
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-fast-retrans

The **set protocols vrrp interface vrid ipv6-nd ra-fast-retrans** command can be used to enable or disable IPv6 nd ra-fast-retrans.

The **delete protocols vrrp interface vrid ipv6-nd ra-fast-retrans** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-fast-retrans** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ra-fast-retrans <**true	false**>	Enable or disable IPv6 nd ra-fast-retrans. • **true**: Enable IPv6 nd ra-fast-retrans. • **false**: Disable IPv6 nd ra-fast-retrans. By default, IPv6 nd ra-fast-retrans is enabled.

Usage Guidelines

RFC4861 states that consecutive RA packets should be sent no more frequently than three seconds apart. FRR by default allows faster transmissions of RA packets in order to speed convergence and neighbor establishment, particularly for unnumbered peering. By turning off ipv6 nd ra-fast-retrans, the implementation is compliant with the RFC at the cost of slower convergence and neighbor establishment.

Example

- Disable IPv6 nd ra-fast-retrans.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-fast-retrans false
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-interval

The **set protocols vrrp interface vrid ipv6-nd ra-interval** command configures the maximum time allowed between sending unsolicited multicast router advertisements from the interface.

The **delete protocols vrrp interface vrid ipv6-nd ra-interval** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-interval** {**msec** <*interval1*> **| sec** <*interval2*>}

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
msec <*interval1*>	Specifies the maximum time between sending unsolicited multicast router advertisements from the interface in milliseconds. The value is an integer that ranges from 70 to 1800000. Default: 600000.
sec <*interval2*>	Specifies the maximum time between sending unsolicited multicast router advertisements from the interface in seconds. The value is an integer that ranges from 1 to 1800. Default: 600.

Example

- Configure the maximum time allowed between sending unsolicited multicast router advertisements from the interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-interval msec 600000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-lifetime

The **set protocols vrrp interface vrid ipv6-nd ra-lifetime** command configures the lifetime, in seconds, for the routing switch to be used as a default router by hosts on the current interface.

The **delete protocols vrrp interface vrid ipv6-nd ra-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-lifetime** <*time*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ra-lifetime <*time*>	Specifies lifetime in seconds of a default router. A setting of 0 for default router lifetime in an RA indicates that the routing switch is not a default router on the interface. Range: 0-9000 seconds. Default: 1800 seconds.

Example

- Configure the lifetime for the routing switch to be used as a default router by hosts on the current interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-lifetime 2000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd reachable-time

The **set protocols vrrp interface vrid ipv6-nd reachable-time** command configures the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The **delete protocols vrrp interface vrid ipv6-nd reachable-time** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd reachable-time** <*time*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
reachable-time <*time*>	Specifies the reachable time in milliseconds. Range: 1-3600000. Default: 0 (no limit).

Example

- Configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd reachable-time 2000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd router-preference

The **set protocols vrrp interface vrid ipv6-nd router-preference** command specifies the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs) that the switch sends from an interface. An interface with a DRP value of high will be preferred by other devices on the network over interfaces with an RA value of medium or low.

The **delete protocols vrrp interface vrid ipv6-nd router-preference** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd router-preference** <**high | medium | low**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
router-preference <**high	medium	low**>	Specifies the value that is set in the Default Router Preference (DRP) field. • **high**: Sets DRP to high. • **medium**: Sets DRP to medium. Default. • **low**: Sets DRP to low.

Example

- Configure the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs).

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd router-preference high
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd suppress-ra

The **set protocols vrrp interface vrid ipv6-nd suppress-ra** command can be used to enable or disable sending Router Advertisement (RA) on specified VRRP interface. By default, PICOS do not send RA packets on VRRP interfaces.

The **delete protocols vrrp interface vrid ipv6-nd suppress-ra** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd suppress-ra** <**true | false**>

delete protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd suppress-ra**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
<**true	false**>	Enable or disable sending RA packets on specified interface. The value could be **true** or **false**. • **true**: Disables sending RA packets. • **false**: Enables sending RA packets. By default, PICOS do not send RA packets on VRRP interfaces.

Example

- Enable sending RA packets on VLAN interface vlan10.

```
admin@Xorplus# set protocols vrrp interface vlan10 vrid 32 ipv6-nd suppress-ra false
admin@Xorplus# commit
```

Spanning Tree Protocol Commands

- run show spanning-tree
- run show spanning-tree mstp
- run show spanning-tree pvst
- run show spanning-tree rstp
- run show spanning-tree statistics
- run show spanning-tree stp
- set protocols spanning-tree enable
- set protocols spanning-tree force-version
- set protocols spanning-tree interface enable
- set protocols spanning-tree mstp bridge-priority
- set protocols spanning-tree mstp configuration-name
- set protocols spanning-tree mstp forward-delay
- set protocols spanning-tree mstp hello-time
- set protocols spanning-tree mstp interface bpdu-filter
- set protocols spanning-tree mstp interface bpdu-guard
- set protocols spanning-tree mstp interface edge
- set protocols spanning-tree mstp interface external-path-cost
- set protocols spanning-tree mstp interface internal-path-cost
- set protocols spanning-tree mstp interface manual-forwarding
- set protocols spanning-tree mstp interface mode
- set protocols spanning-tree mstp interface port-priority
- set protocols spanning-tree mstp interface root-guard
- set protocols spanning-tree mstp interface tcn-guard
- set protocols spanning-tree mstp max-age
- set protocols spanning-tree mstp max-hops
- set protocols spanning-tree mstp msti bridge-priority
- set protocols spanning-tree mstp msti interface cost
- set protocols spanning-tree mstp msti interface port-priority
- set protocols spanning-tree mstp revision-level
- set protocols spanning-tree mstp msti vlan
- set protocols spanning-tree pvst interface bpdu-guard
- set protocols spanning-tree pvst interface manual-forwarding
- set protocols spanning-tree pvst interface mode
- set protocols spanning-tree pvst interface root-guard
- set protocols spanning-tree pvst vlan bridge-priority
- set protocols spanning-tree pvst vlan enable
- set protocols spanning-tree pvst vlan forward-delay
- set protocols spanning-tree pvst vlan hello-time
- set protocols spanning-tree pvst vlan interface path-cost
- set protocols spanning-tree pvst vlan interface port-priority
- set protocols spanning-tree pvst vlan max-age
- set protocols spanning-tree rstp bridge-priority
- set protocols spanning-tree rstp forward-delay
- set protocols spanning-tree rstp hello-time
- set protocols spanning-tree rstp interface bpdu-filter
- set protocols spanning-tree rstp interface bpdu-guard
- set protocols spanning-tree rstp interface edge
- set protocols spanning-tree rstp interface mode
- set protocols spanning-tree rstp interface path-cost
- set protocols spanning-tree rstp interface port-priority
- set protocols spanning-tree rstp interface root-guard
- set protocols spanning-tree rstp interface tcn-guard
- set protocols spanning-tree rstp max-age
- set protocols spanning-tree stp bridge-priority
- set protocols spanning-tree stp forward-delay
- set protocols spanning-tree stp hello-time
- set protocols spanning-tree stp interface bpdu-filter
- set protocols spanning-tree stp interface bpdu-guard
- set protocols spanning-tree stp interface edge
- set protocols spanning-tree stp interface mode
- set protocols spanning-tree stp interface path-cost
- set protocols spanning-tree stp interface port-priority
- set protocols spanning-tree stp interface root-guard

- set protocols spanning-tree stp interface tcn-guard
- set protocols spanning-tree stp max-age

run show spanning-tree

The **run show spanning-tree** command displays the configuration information and status of spanning tree.

Command Syntax

run show spanning-tree

Parameter

None.

Example

- Run **run show spanning-tree** command to view the configuration information and status of spanning tree.

```
admin@PICOS# run show spanning-tree
-------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: MSTP
  Root ID: 32768.3c:2c:30:10:20:83
  External Root Path Cost: 0
  CIST Regional Root ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  CIST Internal Root Path Cost: 800
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 19
  Bridge Configuration Name: Pica8
  Bridge Revision Level: 0
  Bridge Configuration Digest: ac36177f50283cd4b83821d8ab26de62
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:00:56
Local Parameters
  Bridge ID: 32768.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 20
```

run show spanning-tree mstp

The **run show spanning-tree mstp** command displays the configuration information and status of spanning tree protocol MSTP.

Command Syntax

run show spanning-tree mstp <**bridge** | **interface**> [**all** | **cist** | **msti** <*msti_num*>]

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.
[**all** | **cist** | **msti** <*msti_num*>]	Optional. The value could be **all**, **cist** or **msti** <*msti_num*>. • **all**: Indicates to show the MSTP information of all the MSTIs. • **cist**: Indicates to show the MSTP information of CIST. • **msti** <*msti_num*>: Specifies the MST instance number. Indicates to show the MSTP information of a specific MSTI.

Example

- Run **run show spanning-tree mstp** command to view the configuration information and status of spanning tree protocol MSTP.

```
admin@PICOS# run show spanning-tree mstp bridge all
--------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: MSTP
  Root ID: 32768.3c:2c:30:10:20:83
  External Root Path Cost: 0
  CIST Regional Root ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  CIST Internal Root Path Cost: 800
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 19
  Bridge Configuration Name: Pica8
  Bridge Revision Level: 0
  Bridge Configuration Digest: ac36177f50283cd4b83821d8ab26de62
  Msti 2 Member VLANs:
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:04:31
Local Parameters
  Bridge ID: 32768.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 20
--------------------------------------------------
STP Bridge Parameters for MSTI 2
  MSTI Regional Root: 32770.8c:ea:1b:32:1f:58
  Root Cost: 0
  Root Port:
  Hello Time: 2
  Max Age: 20
  Forward Delay: 15
  Remaining Hops: 20
  Time Since Last Topology Change: 0 day 00:05:15
Local Parameters
  Bridge ID: 32770.8c:ea:1b:32:1f:58
```

run show spanning-tree pvst

The **run show spanning-tree pvst** command displays the configuration information and status of spanning tree protocol Rapid PVST+.

Command Syntax

run show spanning-tree pvst <**bridge** | **interface**> [**all** | **vlan** <*vlan-id*>]

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**. The value could be **all**, **vlan** <*vlan-id*>.
[**all** | **vlan** <*vlan-id*>]	• **all**: Indicates to show the Rapid PVST+ information of all the VLANs. • **vlan** <*vlan-id*>: Specifies the VLAN ID. Indicates to show the Rapid PVST+ information of a specific VLAN. Optional when showing the spanning tree information based on **bridge**. Required when showing the spanning tree information based on **interface**.

Example

- Run **run show spanning-tree pvst** command to view the configuration information and status of spanning tree protocol Rapid PVST+.

```
admin@PICOS# run show spanning-tree pvst interface all

Rapid PVST+ Spanning Tree Interface Status for VLAN 1
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  -----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        FORWARDING  ROOT


admin@PICOS# run show spanning-tree pvst bridge
------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: PVST
  Root ID: 32768.3c:2c:30:10:20:83
  Root Path Cost: 800
  Designated Bridge ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:00:35
Local Parameters
  Bridge ID: 32769.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
```

run show spanning-tree rstp

The **run show spanning-tree rstp** command displays the configuration information and status of spanning tree protocol RSTP.

Command Syntax

run show spanning-tree rstp <**bridge** | **interface**>

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.

Example

- Run **run show spanning-tree rstp** command to view the configuration information and status of spanning tree protocol RSTP.

```
admin@PICOS# run show spanning-tree rstp interface

RSTP Spanning Tree Interface Status
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  ----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        FORWARDING  ROOT
```

run show spanning-tree statistics

The **run show spanning-tree statistics** command displays the statistics information of spanning tree.

Command Syntax

run show spanning-tree statistics [**interface** <*interface-name*>]

Parameter

Parameter	Description
<*interface-name*>	Optional. Specifies a interface name. It can be a physical interface or a LAG interface. Use this parameter to show the spanning tree statistics information of a specific interface.

Example

- Run **run show spanning-tree statistics** command to view the statistics information of spanning tree.

```
admin@PICOS# run show spanning-tree statistics
Interface   BPDU Rx Count  BPDU Tx Count
----------  -------------  -------------
te-1/1/1    173            50
```

run show spanning-tree stp

The **run show spanning-tree stp** command displays the configuration information and status of spanning tree protocol STP.

Command Syntax

run show spanning-tree stp <**bridge** | **interface**>

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.

Example

- Run **run show spanning-tree stp** command to view the configuration information and status of spanning tree protocol STP.

```
admin@PICOS# run show spanning-tree stp interface

STP Spanning Tree Interface Status
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  ----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        DISCARDING  ROOT
```

set protocols spanning-tree enable

The **set protocols spanning-tree enable** command is used to enable or disable spanning tree protocols on a switching device.

Command Syntax

set protocols spanning-tree enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true	false**>	Enables or disables spanning tree protocols. The value could be **true** or **false**. • **true**: enables spanning tree protocols. • **false**: disables spanning tree protocols. By default, spanning tree protocols is enabled.

Usage Guidelines

To enable a spanning tree protocol, use the **set protocols spanning-tree enable true** command first, then use the **set protocols spanning-tree force-version** <**0** | **2** | **3** | **4**> command to specify the protocol version.

Note: To enable Rapid-PVST+, you must also enable Rapid-PVST+ on the VLAN by using the **set protocols spanning-tree pvst vlan** <*vlan-id*> **enable true** command.

Example

- Disable spanning tree protocols.

```
admin@Xorplus# set protocols spanning-tree enable false
admin@Xorplus# commit
```

- Enable spanning tree protocols.

```
admin@Xorplus# set protocols spanning-tree enable true
admin@Xorplus# commit
```

set protocols spanning-tree force-version

The **set protocols spanning-tree force-version** command sets the version of the spanning tree protocol on a switching device.

Command Syntax

set protocols spanning-tree force-version <**0 | 2 | 3 | 4**>

Parameter

Parameter	Description
force-version <**0** | **2**| **3** | **4**>	Specifies the version of the spanning tree protocol. The value could be **0**, **2**, **3** or **4**. • **0**: Indicates the STP mode. • **2**: Indicates the RSTP mode. • **3**: Indicates the MSTP mode. • **4**: Indicates the Rapid-PVST+ mode. The default spanning tree protocol is MSTP.

Usage Guidelines

A switch has four operation modes: Rapid-PVST+, MSTP, RSTP, and STP. On the network running a spanning tree protocol, switches running different spanning tree protocols cannot communicate with each other. As a result, spanning trees cannot be properly calculated.

Example

- Set the version of the spanning tree protocol to Rapid-PVST+.

```
admin@Xorplus# set protocols spanning-tree force-version 4
admin@Xorplus# commit
```

set protocols spanning-tree interface enable

The **set protocols spanning-tree interface enable** command can be used to enable or disable spanning tree protocol on a specific interface.

The **delete protocols spanning-tree interface enable** command deletes the configuration.

Command Syntax

set protocols spanning-tree interface <*interface-name*> **enable** <**true | false**>

delete protocols spanning-tree interface <*interface-name*> **enable**

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value is a physical port or an LAG port.
enable <**true	false**>	Enable or disable spanning tree protocol on a specific interface. The value could be **true** or **false**. • **true**: Enable spanning tree protocol. • **false**: Disable spanning tree protocol. By default, spanning tree protocol is enabled.

Example

- Disable spanning tree protocol on interface te-1/1/7.

```
admin@PICOS# set protocols spanning-tree interface te-1/1/7 enable false
admin@PICOS# commit
```

set protocols spanning-tree mstp bridge-priority

The **set protocols spanning-tree mstp bridge-priority** command sets the bridge priority of the switching device when MSTP is running.

Command Syntax

set protocols spanning-tree mstp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when MSTP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp configuration-name

The **set protocols spanning-tree mstp configuration-name** command configures the MST region name of the switching device.

Command Syntax

set protocols spanning-tree mstp configuration-name <*configuration-name*>

Parameter

Parameter	Description
configuration-name <*configuration-name*>	Specifies the MST region name. The value is a string.

Usage Guidelines

MST region name is used to distinguish MST regions. Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

Example

- Configure the MSTP bridge configuration name.

```
admin@Xorplus# set protocols spanning-tree mstp configuration-name mstp1
admin@Xorplus# commit
```

set protocols spanning-tree mstp forward-delay

The **set protocols spanning-tree mstp forward-delay** command sets the value of the MSTP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree mstp forward-delay <*forward-delay*>

Parameter

Parameter	Description
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the MSTP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree mstp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree mstp hello-time

The **set protocols spanning-tree mstp hello-time** command sets the interval of the switching device to send BPDUs when MSTP is running.

Command Syntax

set protocols spanning-tree mstp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface bpdu-filter

The **set protocols spanning-tree mstp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **bpdu-filter** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true**	**false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

> **NOTE:**
>
> If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface bpdu-guard

The **set protocols spanning-tree mstp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree mstp interface** <*interface-name*> **bpdu-guard** true command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** command manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface edge

The **set protocols spanning-tree mstp interface edge** command configures a physical port or a LAG port as an edge port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. The default value is false.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface external-path-cost

The **set protocols spanning-tree mstp interface external-path-cost** command configures the path cost of the external link on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **external-path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
external-path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

External path cost indicates the path cost from a CIST regional root to the root. External path cost saved on all switching devices in an MST region are same. If the CIST root is in an MST region, external path cost saved on all switching devices in the MST region are 0s.

Note: When the path cost value changes, the spanning tree will be recalculated.

Example

- Configure the path cost of the external link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 external-path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface internal-path-cost

The **set protocols spanning-tree mstp interface internal-path-cost** command configures the path cost of the internal link on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **internal-path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
internal-path-cost <*path-cost*>	Specifies the path cost value of the internal link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Indicates the path cost from the local bridge to the regional root. The internal path cost saved on a regional edge port is greater than that saved on a non-regional edge port.

Example

- Configure the path cost of the internal link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 internal-path-cost 1248
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface manual-forwarding

The **set protocols spanning-tree mstp interface manual-forwarding** command manually configures a physical port or a LAG port as a forwarding port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **manual-forwarding** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
manual-forwarding <**true** | **false**>	Manually configure a physical port or a LAG port as a forwarding port. The value could be **true** or **false**. • **true**: manually configures a physical port or a LAG port as a forwarding port. • **false**: disables manual forwarding on a port. By default, manual forwarding is disabled.

Usage Guidelines

After manually configuring a physical port or a LAG port as a forwarding port, the state of the port is always forwarding, unless the port is down. The port does not participate in spanning tree calculation and does not send and receive BPDUs.

Example

- Configure the port ge-1/1/1 as a forwarding port manually for MSTP mode.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 manual-forwarding true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface mode

The **set protocols spanning-tree mstp interface mode** command configures the link type of a port. The setting for port duplex mode applies to this port on all MST instances.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point** | **shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface port-priority

The **set protocols spanning-tree mstp interface port-priority** command configures the priority of a port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface root-guard

The **set protocols spanning-tree mstp interface root-guard** command is used to enable or disable root guard function for MSTP.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true**	**false**>	Enables or disables root guard function for MSTP. The value could be **true** or **false**. • **true**: enables root guard function for MSTP. • **false**: disables root guard function for MSTP. By default, root guard function for MSTP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for MSTP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 root-guard true
```

set protocols spanning-tree mstp interface tcn-guard

The **set protocols spanning-tree mstp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for MSTP mode.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree mstp max-age

The **set protocols spanning-tree mstp max-age** command sets the BPDU aging time on the switching device when MSTP is running.

Command Syntax

set protocols spanning-tree mstp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of a received BPDU packets. If the BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp max-hops

The **set protocols spanning-tree mstp max-hops** command sets the maximum hops of a spanning tree when MSTP is running.

Command Syntax

set protocols spanning-tree mstp max-hops <*max-hops*>

Parameter

Parameter	Description
max-hops <*max-hops*>	Specifies the maximum hops of a spanning tree. The value is an integer that ranges from 6 to 40. The default value is 20.

Usage Guidelines

The maximum number of hops of a spanning tree in an MST region determines the network scale.

An MST BPDU has a field that indicates the number of remaining hops:

- The number of remaining hops in a BPDU sent by the root switching device equals the maximum number of hops.
- The number of remaining hops in a BPDU sent by a non-root switching device equals the maximum number of hops minus the number of hops from the non-root switching device to the root switching device.
- If a switching device receives a BPDU in which the number of remaining hops is 0, the switching device will discard the BPDU.

Example

- Set the maximum hops of a spanning tree to 15 when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp max-hops 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti bridge-priority

The **set protocols spanning-tree mstp msti bridge-priority** command sets the bridge priority for an MSTI of the switching device.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **bridge-priority** <*bridge-priority*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16. Each process supports a maximum of 16 instances.
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device for an MSTI. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority of the switching device to 55 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti interface cost

The **set protocols spanning-tree mstp msti interface cost** command configures the path cost of the link on a physical port or a LAG port for an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **interface** <*interface-name*> **cost** <*cost-value*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
cost <*cost-value*>	Specifies the path cost of an interface. The value is an integer ranges from 0 to 200000000. The default value is 0.

Example

- Set the path cost of ge-1/1/1 to 556 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 interface ge-1/1/1 cost 556
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti interface port-priority

The **set protocols spanning-tree mstp msti interface port-priority** command configures the port priority for an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **interface** <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Set the bridge priority of interface ge-1/1/1 to 55 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 interface ge-1/1/1 port-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp revision-level

The **set protocols spanning-tree mstp revision-level** command sets the revision level of the MST region.

Command Syntax

set protocols spanning-tree mstp revision-level <*level*>

Parameter

Parameter	Description
revision-level <*level*>	Specifies the revision level of the MST region. The value is an integer that ranges from 0 to 65535. The default value is 0.

Usage Guidelines

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST configuration name
- Mappings between MSTIs and VLANs
- MST region revision level

MSTP is a standard protocol, the MSTP revision level of a switching device is 0 by default. If the revision level of some devices from a specified manufacturer is not 0, you must change the MSTP revision level of devices to be the same to compatible with the spanning tree calculation in an MST region.

Example

- Set the MSTP revision level of the switching device to 5.

```
admin@Xorplus# set protocols spanning-tree mstp revision-level 5
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti vlan

The **set protocols spanning-tree mstp vlan** command adds a VLAN to an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **vlan** <*vlan-id*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094. e.g. 2,3,5-100.

Usage Guidelines

The MSTIs are independent of each other, and the MSTI can correspond to one or more VLANs. However, a VLAN can only correspond to one MSTI. By default, all VLANs in the MST region are mapped to instance 0.

Example

- Add VLAN 100 to MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 vlan 100
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface bpdu-guard

The **set protocols spanning-tree pvst interface bpdu-guard** command configures BPDU-guard on a physical port or a LAG port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard** true command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Enable BPDU-guard on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface manual-forwarding

The **set protocols spanning-tree pvst interface manual-forwarding** command manually configures a physical port or a LAG port as a forwarding port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **manual-forwarding** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
manual-forwarding <**true	false**>	Manually configure a physical port or a LAG port as a forwarding port. The value could be **true** or **false**. • **true**: manually configures a physical port or a LAG port as a forwarding port. • **false**: disables manual forwarding on a port. By default, manual forwarding is disabled.

Usage Guidelines

After manually configuring a physical port or a LAG port as a forwarding port, the state of the port is always forwarding, unless the port is down. The port does not participate in spanning tree calculation and does not send and receive BPDUs.

Example

- Configure the port ge-1/1/1 as a forwarding port manually for Rapid-PVST+ mode.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 manual-forwarding true
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface mode

The **set protocols spanning-tree pvst interface mode** command configures the link type of a port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface root-guard

The **set protocols spanning-tree pvst interface root-guard** command is used to enable or disable root guard function for Rapid-PVST+.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
root-guard <**true**	**false**>	Enables or disables root guard function for Rapid-PVST+. The value could be **true** or **false**. • **true**: enables root guard function for Rapid-PVST+. • **false**: disables root guard function for Rapid-PVST+. By default, root guard function is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for Rapid-PVST+ mode on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 root-guard true
```

set protocols spanning-tree pvst vlan bridge-priority

The **set protocols spanning-tree pvst vlan bridge-priority** command sets the bridge priority the switching device when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **bridge-priority** <*bridge-priority*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094. A total of 64 VLANs can be enabled for Rapid-PVST+.
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device for Rapid-PVST+ mode. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 for Rapid-PVST+.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan enable

The **set protocols spanning-tree pvst vlan enable** command is used to enable or disable Rapid-PVST+ VLAN instance.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **enable** <**true | false**>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true	false**>	Enables or disables Rapid-PVST+ VLAN instance. The value could be **true** or **false**. • **true**: enables Rapid-PVST+ VLAN instance. • **false**: disables Rapid-PVST+ VLAN instance. By default, Rapid-PVST+ is disabled.

Usage Guidelines

To enable the Rapid-PVST+ protocol, in addition to setting the spanning tree protocol to 4 by using the **set protocols spanning-tree force-version 4** command, Rapid-PVST+ must be enabled on the VLAN.

Example

- Enable Rapid-PVST+ in VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan forward-delay

The **set protocols spanning-tree pvst vlan forward-delay** command sets the value of the Rapid-PVST+ forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **forward-delay** <*forward-delay*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the Rapid-PVST+ forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan hello-time

The **set protocols spanning-tree pvst vlan hello-time** command sets the interval of the switching device to send BPDUs when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **hello-time** <*hello-time*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when Rapid-PVST+ is running.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan interface path-cost

The **set protocols spanning-tree pvst vlan interface path-cost** command configures the link path cost of a physical port or a LAG port in Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **interface** <*interface-name*> **path-cost** <*cost-value*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies a interface name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*cost-value*>	Specifies the path cost of an interface. The value is an integer ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Set the path cost of the switching device to 55 for VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 interface ge-1/1/1 path-cost 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan interface port-priority

The **set protocols spanning-tree pvst vlan interface port-priority** command configures the port priority of an interface in Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **interface** <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

In Rapid-PVST+ spanning tree calculation, the port path cost, bridge ID of the sending switch, and port priority determine whether the port can be selected as the designated port. A smaller priority value indicates higher probability of becoming the designated port, and a larger priority value indicates higher probability of becoming the blocking port.

On a network running Rapid-PVST+, a port can function as different roles in different spanning trees so that traffic from different VLANs is forwarded through different physical paths.

Example

- Set the port priority of the switching device to 55 for VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 interface ge-1/1/1 port-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan max-age

The **set protocols spanning-tree pvst vlan max-age** command sets the BPDU aging time on the switching device when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **max-age** <*max-age*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when Rapid-PVST+ is running.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree rstp bridge-priority

The **set protocols spanning-tree rstp bridge-priority** command sets the bridge priority the switching device when RSTP is running.

Command Syntax

set protocols spanning-tree rstp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when RSTP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree rstp forward-delay

The **set protocols spanning-tree rstp forward-delay** command sets the value of the RSTP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree rstp forward-delay *<forward-delay>*

Parameter

Parameter	Description
forward-delay *<forward-delay>*	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the RSTP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree rstp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree rstp hello-time

The **set protocols spanning-tree rstp hello-time** command sets the interval of the switching device to send BPDUs when RSTP is running.

Command Syntax

set protocols spanning-tree rstp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface bpdu-filter

The **set protocols spanning-tree rstp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **bpdu-filter** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true	false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

> **NOTE:**
>
> If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface bpdu-guard

The **set protocols spanning-tree rstp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard true** command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface edge

The **set protocols spanning-tree rstp interface edge** command configures a physical port or a LAG port as an edge port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. By default, edge port is disabled.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface mode

The **set protocols spanning-tree rstp interface mode** command configures the link type of the port.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or shared. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface path-cost

The **set protocols spanning-tree rstp interface path-cost** command configures the link path cost of a physical port or a LAG port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Configure the path cost of port ge-1/1/1 to 500.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface port-priority

The **set protocols spanning-tree rstp interface port-priority** command configures the priority of a port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface root-guard

The **set protocols spanning-tree rstp interface root-guard** command is used to enable or disable root guard function for RSTP.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true**	**false**>	Enables or disables root guard function for RSTP. The value could be **true** or **false**. • **true**: enables root guard function for RSTP. • **false**: disables root guard function for RSTP. By default, root guard function for RSTP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for RSTP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 root-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface tcn-guard

The **set protocols spanning-tree rstp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for RSTP mode.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp max-age

The **set protocols spanning-tree rstp max-age** command sets the BPDU aging time on the switching device when RSTP is running.

Command Syntax

set protocols spanning-tree rstp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree stp bridge-priority

The **set protocols spanning-tree stp bridge-priority** command sets the bridge priority the switching device when STP is running.

Command Syntax

set protocols spanning-tree stp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when STP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree stp forward-delay

The **set protocols spanning-tree stp forward-delay** command sets the value of the STP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree stp forward-delay <*forward-delay*>

Parameter

Parameter	Description
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the STP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree stp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree stp hello-time

The **set protocols spanning-tree stp hello-time** command sets the interval of the switching device to send BPDUs when STP is running.

Command Syntax

set protocols spanning-tree stp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree stp interface bpdu-filter

The **set protocols spanning-tree stp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **bpdu-filter** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true	false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

> **NOTE:**
>
> If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface bpdu-guard

The **set protocols spanning-tree stp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard true** command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface edge

The **set protocols spanning-tree stp interface edge** command configures a physical port or a LAG port as an edge port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. By default, edge port is disabled.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface mode

The **set protocols spanning-tree stp interface mode** command configures the link type of the port.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree stp interface path-cost

The **set protocols spanning-tree stp interface path-cost** command configures the link path cost of a physical port or a LAG port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Configure the path cost of the external link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree stp interface port-priority

The **set protocols spanning-tree stp interface port-priority** command configures the priority of a port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree stp interface root-guard

The **set protocols spanning-tree stp interface root-guard** command is used to enable or disable root guard function for STP.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true** | **false**>	Enables or disables root guard function for STP. The value could be **true** or **false**. • **true**: enables root guard function for STP. • **false**: disables root guard function for STP. By default, root guard function for STP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for STP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 root-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface tcn-guard

The **set protocols spanning-tree stp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for STP mode.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp max-age

The **set protocols spanning-tree stp max-age** command sets the BPDU aging time on the switching device when STP is running.

Command Syntax

set protocols spanning-tree stp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp max-age 15
admin@Xorplus# commit
```

MLAG Commands

- set protocols mlag domain
- set protocols mlag domain node
- set protocols mlag domain interface link
- set protocols mlag domain peer-ip peer-link
- set protocols mlag domain peer-ip peer-vlan
- run show mlag domain
- run show mlag link
- run show mlag consistency-parameter

set protocols mlag domain

The **set protocols mlag domain** command creates an MLAG domain ID.

Command Syntax

set protocols mlag domain <*domain-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.

Example

- Create an MLAG domain.

```
admin@Xorplus# set protocols mlag domain 3
admin@Xorplus# commit
```

set protocols mlag domain node

The **set protocols mlag domain node** command specifies the node ID for the MLAG device.

Command Syntax

set protocols mlag domain <*domain-id*> **node** <**0 | 1**>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
node <**0	1**>	Specifies the node ID for the MLAG device. The value could be **0** or **1**.

Example

- Set the node ID for the MLAG device as 0.

```
admin@Xorplus# set protocols mlag domain 3 node 0
admin@Xorplus# commit
```

set protocols mlag domain interface link

The **set protocols mlag domain interface link** command configures the link ID on the MLAG member port.

Command Syntax

set protocols mlag domain <*domain-id*> **interface** <*lag-interface*> **link** <*link-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
interface <*lag-interface*>	Specifies the MLAG member port. The value is a LAG interface.
link <*link-id*>	Specifies the link ID. The value is an integer that ranges from 1 to 255.

Example

- Configure the link ID to 2 on MLAG member port ae3.

```
admin@Xorplus# set protocols mlag domain 3 interface ae3 link 2
admin@Xorplus# commit
```

set protocols mlag domain peer-ip peer-link

The **set protocols mlag domain peer-ip peer-link** command configures peer IP address and peer link port.

Command Syntax

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-link** <*peer-interface-name*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
peer-ip <*peer-ipv4-address*>	The IP address of the remote MLAG peer link port. The value is in dotted decimal notation.
peer-link <*peer-interface-name* >	The interface name of the peer link that is on the peer device, it should be a LAG port.

Example

- Configure peer IP address and peer link port.

```
admin@Xorplus# set interface mlag domain 3 peer-ip 10.10.10.1 peer-link ae1
admin@Xorplus# commit
```

set protocols mlag domain peer-ip peer-vlan

The **set protocols mlag domain peer-ip peer-vlan** command configures an MLAG peer VLAN.

Command Syntax

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-vlan** <*vlan-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
peer-ip <*peer-ipv4-address*>	The IP address of the remote MLAG peer-link port. The value is in dotted decimal notation.
peer-vlan <*vlan-id*>	Specifies a peer VLAN ID. The value is an integer that ranges from 1 to 4094. The recommended value is 4088.

Usage Guidelines

A specified VLAN MUST be assigned to the peer-link interface, the MLAG peer VLAN, which is dedicated to transmitting MLAG control plane messages but does not allow data messages.

Example

- Configure a peer VLAN for MLAG.

```
admin@Xorplus# set l3-interface vlan-interface vlan4088 address 10.10.10.24 prefix-length 24
admin@Xorplus# set protocols mlag domain 2 peer-ip 10.10.10.1 peer-link ae2
admin@Xorplus# set interface mlag domain 2 peer-ip 10.10.10.1 peer-vlan 4088
admin@Xorplus# commit
```

run show mlag domain

The **run show mlag domain** command displays the global MLAG domain information.

Command Syntax

run show mlag domain {<*domain-id*>| **summary**}

Parameter

Parameter	Description
<*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
summary	Show all MLAG information for all the MLAG domains. Currently, only one domain is supported on one MLAG device.

Example

- Show the global MLAG domain information.

```
admin@Xorplus# run show mlag domain summary
Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 0
-------------------------------------------------------------------------------
Peer Link  Peer IP  Peer Vlan  Neighbor     Status  Config Matched  MAC Synced  # of Links
---------  -------  ---------  ---------  ----------    ---------    ---------    -------
ae23       1.1.1.2    4088    ESTABLISHED      Yes       Yes                      2
```

Table 1. Description of the run show mlag domain command output

Item	Description
Domain-ID	Indicates the MLAG domain ID.
Domain-MAC	Indicates the MLAG domain MAC of MLAG device.
Node-ID	Indicates Node ID of the local MLAG device.
Peer-Link	Indicates the local peer-link port.
Peer-IP	Indicates IP address of the remote peer-link port.
Peer Vlan	Indicates the MLAG peer VLAN.
Neighbor Status	Indicates MLAG neighbor status, the value could be IDLE, CONNECTING, ESTABLISHED.
Config Matched	Indicates the consistency check results, the value could be **Yes** or **No**. When all the check items in the configuration consistency check list in 1.1.6 Configuration Consistency Check are consistent, including **Global configuration** and **Per MLAG configuration**, then it is displayed as **Yes**, otherwise it is **No**.
MAC Synced	Indicates whether MAC synchronization is performed between the MLAG peer devices, the value could be **Yes** or **No**. When both the following conditions match, it displays **Yes**, indicating that the MLAG MAC Sync function is normal between the two MLAG devices: • When "**Neighbor Status**" is ESTABLISHED; • In the result of **run show mlag consistency-parameter link** <*link-id*>, “Port Configurations” are all PASS, and in the result of **run show mlag consistency-parameter summary**, “MLAG Configurations” are all PASS. If any of the above conditions is not satisfied, **No** is displayed, indicating that MAC sync has stopped between the MLAG peers.
# of Links	Indicates numbers of MLAG.

run show mlag link

The **run show mlag link** command displays MLAG link information.

Command Syntax

run show mlag link {*<link-id>*| **summary**}

Parameter

Parameter	Description
<link-id>	Specifies the MLAG link ID to show the specific MLAG information.
summary	Show MLAG information for all the MLAG links.

Example

- Show the MLAG link information.

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   --------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

Table 1. Description of the run show mlag link command output

Item	Description
Link	Indicates the link ID of each MLAG.
Local LAG	Indicates the MLAG member port number on local MLAG device.
Link Status	Indicates MLAG interface state, the value could be INIT, IDLE, DOWN, STANDBY, AS_DOWN, AS_PEER, AS_LOCAL or FULL.
Local Status	Indicates the status of local MLAG member port, the value could be UP, DOWN or UNKNOWN.
Peer Status	Indicates the status of remote MLAG member port, the value could be UP, DOWN or UNKNOWN.
Config Matched	Indicates the consistency check results, the value could be Yes or No.
Flood	Indicates whether traffic received on the MLAG peer-link cannot be transferred through the MLAG member port. The value could be **Yes** or **No**. • **Yes**: indicates that traffic received on the MLAG peer-link can be transferred through the MLAG member port. This happens only in the case when peer MLAG member port is down, the MLAG interface state changes to AS_LOCAL. • **No**: indicates that traffic received on the MLAG peer-link cannot be transferred through the MLAG member port.

run show mlag consistency-parameter

The **run show mlag consistency-parameter** command displays the result of MLAG configuration consistency check, including the global and per MLAG configuration.

Command Syntax

run show mlag consistency-parameter { **link** <*link-id*>| **summary**}

Parameter

Parameter	Description
link <*link-id*>	Specifies the MLAG link ID. This displays the result of per MLAG configuration consistency check.
summary	Show the result of global MLAG configuration consistency check.

Example

- Show the result of per MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter link 3
Port Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
MTU                      1514             1514             PASS
Mac Learning             Yes              Yes              PASS
Lag Mode                 LACP             LACP             PASS
Native Vlan              3                3                PASS
Port Vlan Mode           Access           Access           PASS
Trunk Vlan Count         2                2                PASS
Trunk VLAN IDs                                             PASS

Spanning-Tree Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Mode                     PVST             PVST             PASS
BPDU Guard               No               No               PASS
Root Guard               No               No               PASS
Manual Forwarding        No               No               PASS
Link Type                P2P              P2P              PASS
Instance Count           1                1                PASS
Instance Vlan 3

-- Port Priority         128              128              PASS
-- Path Cost             0                0                PASS

VXLAN Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ----
```

- Show the result of global MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS
Link 2  : PASS
Link 3  : PASS

MLAG Configurations:
----------------------------------------------------------------
```

```
Property                  Local Value      Peer Value       Result
------------------------  ---------------  ---------------  ------
Domain ID                 1                1                PASS
Node ID                   1                0                PASS
Peer VLAN                 4088             4088             PASS
Link Count                3                3                PASS
Link IDs                  1   2   3        1   2   3        PASS

Spanning-Tree Configurations:
----------------------------------------------------------------
Property                  Local Value      Peer Value       Result
------------------------  ---------------  ---------------  ------
Enable                    Yes              Yes              PASS
Mode                      PVST             PVST             PASS
Instance Count            65               65               PASS
Instance Vlan 1
-- Bridge Priority        32768            32768            PASS
-- Hello Time             2                2                PASS
-- Forward Delay          15               15               PASS
-- Max Age                20               20               PASS
Instance Vlan 2
-- Bridge Priority        32768            32768            PASS
-- Hello Time             2                2                PASS
-- Forward Delay          15               15               PASS
-- Max Age                20               20               PASS
Instance Vlan 3
-- Bridge Priority        32768            32768            PASS
-- Hello Time             2                2                PASS
-- Forward Delay          15               15               PASS
-- Max Age                20               20               PASS
Instance Vlan 4
-- Bridge Priority        32768            32768            PASS
-- Hello Time             2                2                PASS
-- Forward Delay          15               15               PASS
-- Max Age                20               20               PASS

DHCP Snooping Configurations:
----------------------------------------------------------------
Property                  Local Value      Peer Value       Result
------------------------  ---------------  ---------------  ------
VLAN Count                0                4                FAIL
VLAN IDs                                                    FAIL

IGMP Snooping Configurations:
----------------------------------------------------------------
Property                  Local Value      Peer Value       Result
------------------------  ---------------  ---------------  ------
Enable                    No               No               PASS

VXLAN Configurations:
----------------------------------------------------------------
Property                  Local Value      Peer Value       Result
------------------------  ---------------  ---------------  ------
VXLAN                     N/A              N/A              PASS
VXLAN VNI Count           0                0                PASS
VXLAN VNIs                                                  PASS
```

GRE Tunnel Interface Commands

- run show l3-interface tunnel
- set l3-interface tunnel address
- set l3-interface tunnel destination
- set l3-interface tunnel disable
- set l3-interface tunnel source
- set l3-interface tunnel tunnel-mode gre-ip
- set l3-interface tunnel vrf

run show l3-interface tunnel

To display information about an GRE tunnel interface, use the **run show l3-interface tunnel** command in L2/L3 configuration mode.

> **NOTE:**
> GRE tunnel is a logical interface created by Linux kernel on software side. Once created, GRE tunnel stays in "**UP**" state in the display of this show command. Unless it is shut down by CLI command "**set l3-interface tunnel ddd disable**", the state will change to "**DOWN**".

Command Syntax

run show l3-interface tunnel <*tunnel-interface-name*>

Parameters

Parameter	Description
tunnel <*tunnel-interface-name*>	The GRE tunnel interface name.

Example

- The following example displays information about GRE tunnel interface **tnl1**. In the output information, **Inet addr** indicates the tunnel interface IP address.

```
admin@Xorplus# run show l3-interface tunnel tnl1
tnl1        State:UP
            Tunnel Source: 1.1.1.1
            Tunnel Destnation:: 2.2.2.2
            Tunnel protocol/transport: gre-ip
            Inet addr: 10.1.1.1/24
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................0
              IPv4 Forwarding Packets....................0
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
```

set l3-interface tunnel address

Run the command **set l3-interface tunnel address** to configure a GRE tunnel name and tunnel interface IP address.

Use the command **delete-interface tunnel address** to delete this tunnel from the switch configuration.

> **NOTEs:**
> Note that before committing this configuration, make sure you have configured the tunnel mode as **gre-ip** by using the command **set l3-interface tunnel tunnel-mode.**

Command Syntax

set l3-interface tunnel <*tunnel-name*> **address** <*ip-address*> **prefix-length** <*prefix-length*>

delete l3-interface tunnel <*tunnel-name*> **address** <*ip-address*> **prefix-length**

Parameter

Parameter	Description
tunnel <*tunnel-name*>	Specifies the tunnel name, in alpha-numeric format with no spaces.
address <*ip-address*>	Specifies the tunnel interface IPv4 or IPv6 address.
prefix-length <*prefix-length*>	Specifies the IP prefix length.

Example

- Create a GRE tunnel tn14 and assign 192.168.8.1 as the tunnel interface address with prefix length 24.

```
admin@switch1# set l3-interface tunnel tnl4 address 192.168.8.1 prefix-length 24
admin@switch1# set l3-interface tunnel tnl4 tunnel-mode gre-ip
admin@switch1# commit
```

set l3-interface tunnel destination

Run the command **set l3-interface tunnel destination** to configure the GRE tunnel destination IPv4 address.

Run the command **delete l3-interface tunnel destination** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name***> destination <***IPv4-address***>**

delete l3-interface tunnel <*tunnel-name***> destination**

Parameter

Parameter	Description
tunnel <*tunnel-name***>**	Specifies the name of the tunnel, its value is alpha-numeric with no spaces.
destination <*IPv4-address***>**	Specifies the GRE tunnel destination IP address in IPv4 format.

Example

- Configure the destination GRE tunnel IPv4 address for tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 destination 1.1.1.1
admin@Xorplus# commit
```

set l3-interface tunnel disable

The **set l3-interface tunnel disable** command can be used to enable or disable a GRE tunnel interface.

Command Syntax

set l3-interface tunnel <*tunnel-interface-name*> **disable** <**true | false**>

Parameters

Parameter	Description
tunnel <*tunnel-interface-name*>	Specifies the name of the GRE tunnel interface. The value is a string.
disable <**true	false**>	Enables or disables the GRE tunnel interface. The value could be **true** or **false**. • **true**: Disable the GRE tunnel interface. • **false**: Enable the GRE tunnel interface. When a GRE tunnel interface is created, it is enabled by default.

Example

- Disable GRE tunnel interface tl2.

```
admin@Xorplus# set l3-interface tunnel tl2 disable true
admin@Xorplus# commit
```

set l3-interface tunnel source

Run the command **set l3-interface tunnel source** to configure the GRE tunnel source IPv4 address or source interface.

Run the command **delete l3-interface tunnel source** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name***> source** <*tunnel-source*>

delete l3-interface tunnel <*tunnel-name***> source**

Parameter

Parameter	Description
tunnel <*tunnel-name***>**	Specifies the name of the GRE tunnel in alpha-numeric format with no spaces.
source <*tunnel-source*>	Specifies the GRE tunnel source IPv4 address or source interface. PicOS supports to configure a loopback interface, an L3 VLAN interface, a routed interface or a sub-interface to a GRE tunnel. If multiple IP addresses are configured on the source interface, the smallest IP address will be the source IP address of this GRE tunnel.

Example

- Configure the GRE tunnel source IPv4 address as 2.2.2.2 for tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 source 2.2.2.2
admin@Xorplus# commit
```

set l3-interface tunnel tunnel-mode gre-ip

Run the command **set l3-interface tunnel tunnel-mode gre-ip** to configure the tunnel mode. Currently only GRE tunnel type is supported by PICOS.

To delete this configuration, run the command **delete l3-interface tunnel tnl4 tunnel-mode gre-ip.**

Command Syntax

set l3-interface tunnel <*tunnel-name*> **tunnel-mode gre-ip**

delete l3-interface tunnel <*tunnel-name*> **tunnel-mode**

Parameter

Parameter	Description
tunnel <*tunnel-name*>	Specifies the tunnel name, in alpha numeric format with no spaces.

Example

- Set the tunnel mode of tunnel tnl4 to gre-ip.

```
admin@XorPlus# set l3-interface tunnel tnl4 tunnel-mode gre-ip
admin@Xorplus# commit
```

set l3-interface tunnel vrf

Run the command **set l3-interface tunnel vrf vrf1** to configure the VRF for the GRE tunnel to attach to.

Run the command **delete l3-interface tunnel vrf vrf1** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name*> **vrf** <*vrf-name*>

delete l3-interface tunnel <*tunnel-name***> vrf**

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF for the GRE tunnel to attach to.
tunnel <*tunnel-name*>	Specifies the GRE tunnel name in alpha-numeric format with no spaces.

Example

- Configure the VRF vrf1 for the GRE tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 vrf vrf1
admin@Xorplus# commit
```

GVRP Commands

- set protocols gvrp join-timer
- set protocols gvrp leave-timer
- set protocols gvrp leaveall-timer
- run clear gvrp interface statistics
- run show gvrp interface
- run show gvrp interface statistics
- set protocols gvrp edge-switch
- set protocols gvrp enable
- set protocols gvrp interface enable
- set protocols gvrp traceoptions flag config
- set protocols gvrp traceoptions flag packets

set protocols gvrp join-timer

The **set protocols gvrp join-timer** command configures the join timer duration for GVRP.

The **delete protocols gvrp join-timer** command deletes the configuration.

> **NOTE**s:
> It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp join-timer *<join-timer>*

delete protocols gvrp join-timer

Parameter

Parameter	Description
<join-timer>	Specifies the join timer. The value is an integer in milliseconds that ranges from 100 to 500. The default value is 200 milliseconds.

Example

- Configure the join timer.

```
admin@PICOS# set protocols gvrp join-timer 300
admin@PICOS# commit
```

set protocols gvrp leave-timer

The **set protocols gvrp leave-timer** command configures the leave timer duration for GVRP.

The **delete protocols gvrp leave-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp leave-timer <*leave-timer*>

delete protocols gvrp leave-timer

Parameter

Parameter	Description
<*leave-timer*>	Specifies the leave timer. The value is an integer in milliseconds that ranges from 300 to 1000. The default value is 1000 milliseconds.

Example

- Configure the leave timer.

```
admin@PICOS# set protocols gvrp leave-timer 800
admin@PICOS# commit
```

set protocols gvrp leaveall-timer

The **set protocols gvrp leaveall-timer** command configures the leaveall timer duration for GVRP.

The **delete protocols gvrp leaveall-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp leaveall-timer <*leaveall-timer*>

delete protocols gvrp leaveall-timer

Parameter

Parameter	Description
<*leaveall-timer*>	Specifies the leaveall timer. The value is an integer in seconds that ranges from 10 to 60. The default value is 10 seconds.

Example

- Configure the leaveall timer.

```
admin@PICOS# set protocols gvrp leaveall-timer 50
admin@PICOS# commit
```

run clear gvrp interface statistics

The **run clear gvrp interface statistics** command is used to clear the GVRP packets statistics.

> **NOTE:**
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run clear gvrp interface *<interface-name>* **statistics**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- Clear the statistics information of GVRP.

```
admin@PICOS# run clear gvrp interface te-1/1/7 statistics
admin@PICOS# run show gvrp interface te-1/1/7 statistics
packet_received: 0
packet_sent:    0
```

run show gvrp interface

The **run show gvrp interface** command is used to view GVRP information on a specific interface, including GVRP Status, Registrar State, Timers and VLANs learned by the interface through GVRP.

Command Syntax

run show gvrp interface *<interface-name>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- View the configuration information of GVRP.

```
admin@PICOS# run show gvrp interface te-1/1/21
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
te-1/1/21       1000             10                 200

Port            Vlans Added
te-1/1/21       10, 11
```

run show gvrp interface statistics

The **run show gvrp interface statistics** command is used to view the interface statistics information of GVRP packets on a specific interface.

Command Syntax

run show gvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- View the statistics information of GVRP.

```
admin@PICOS# run show gvrp interface te-1/1/21 statistics
packet_received: 245
packet_sent:     248
```

set protocols gvrp edge-switch

The **set protocols gvrp edge-switch** command can be used to enable or disable GVRP edge-switch function.

The **delete protocols gvrp edge-switch** command deletes the configuration.

> **NOTE:**
> This command can be enabled only on the edge switches.

Command Syntax

set protocols gvrp edge-switch <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP edge-switch function. The value could be **true** or **false**. • **true**: Enable GVRP edge-switch function. • **false**: Disable GVRP edge-switch function. By default, GVRP edge-switch function is disabled.

Example

- Enable GVRP edge-switch function.

```
admin@PICOS# set protocols gvrp edge-switch true
admin@PICOS# commit
```

set protocols gvrp enable

The **set protocols gvrp enable** command can be used to enable or disable GVRP function globally.

The **delete protocols gvrp enable** command deletes the configuration.

> **NOTE:**
> To enable GVRP function, users need to enable GVRP BOTH globally and at the per-interface level. The command **set protocols gvrp interface enable** enables GVRP function on a specific interface.

Command Syntax

set protocols gvrp enable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP function globally. The value could be **true** or **false**. • **true**: Enable GVRP function globally. • **false**: Disable GVRP function globally. By default, GVRP function is disabled.

Example

- Enable GVRP function globally.

```
admin@PICOS# set protocols gvrp enable true
admin@PICOS# commit
```

set protocols gvrp interface enable

The **set protocols gvrp interface enable** command can be used to enable or disable GVRP function on a specific interface.

The **delete protocols gvrp interface enable** command deletes the configuration.

> **NOTE:**
> To enable GVRP function, users need to enable GVRP BOTH globally and at the per-interface level. The command **set protocols gvrp enable** enables GVRP function globally.

Command Syntax

set protocols gvrp interface <*interface-name*> **enable** <**true | false**>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface or a LAG interface.
<**true	false**>	Enable or disable GVRP function on a specific interface. The value could be **true** or **false**. • **true**: Enable GVRP function on a specific interface. • **false**: Disable GVRP function on a specific interface. By default, GVRP function is disabled.

Example

- Enable GVRP function on a specific interface.

```
admin@PICOS# set protocols gvrp interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols gvrp traceoptions flag config

The **set protocols gvrp traceoptions flag config** command can be used to enable or disable GVRP debugging for configuration tracing.

The **delete protocols gvrp traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols gvrp traceoptions flag config disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable GVRP debugging for configuration tracing. • **false**: Enable GVRP debugging for configuration tracing. By default, GVRP debugging for configuration tracing is disabled.

Example

- Enable GVRP debugging for configuration tracing.

```
admin@PICOS# set protocols gvrp traceoptions flag config disable false
admin@PICOS# commit
```

set protocols gvrp traceoptions flag packets

The **set protocols gvrp traceoptions flag packets** command can be used to enable or disable GVRP debugging for received/sent packets event tracing.

The **delete protocols gvrp traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols gvrp traceoptions flag packets disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP debugging for received/sent packets event tracing. The value could be **true** or **false**. • **true**: Disable GVRP debugging for received/sent packets event tracing. • **false**: Enable GVRP debugging for received/sent packets event tracing. By default, GVRP debugging for received/sent packets event tracing is disabled.

Example

- Enable GVRP debugging for received/sent packets event tracing.

```
admin@PICOS# set protocols gvrp traceoptions flag packets disable false
admin@PICOS# commit
```

MVRP Commands

- run clear mvrp interface statistics
- run show mvrp interface
- run show mvrp interface statistics
- set protocols mvrp edge-switch
- set protocols mvrp enable
- set protocols mvrp interface enable
- set protocols mvrp traceoptions flag config
- set protocols mvrp traceoptions flag packets
- set protocols mvrp join-timer
- set protocols mvrp leave-timer
- set protocols mvrp leaveall-timer

run clear mvrp interface statistics

The **run clear mvrp interface statistics** command is used to clear the MVRP packets statistics.

> **NOTE:**
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run clear mvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- Clear the statistics information of MVRP.

```
admin@PICOS# run clear mvrp interface te-1/1/7 statistics
admin@PICOS# run show mvrp interface te-1/1/7 statistics
packet_received: 0
packet_sent:    0
```

run show mvrp interface

The **run show mvrp interface** command is used to view MVRP information on a specific interface, including MVRP Status, Registrar State, Timers and VLANs learned by the interface through MVRP.

Command Syntax

run show mvrp interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- View the configuration information of MVRP.

```
admin@PICOS# run show mvrp interface te-1/1/21
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
te-1/1/21       1000             10                 200

Port            Vlans Added
te-1/1/21       10, 11
```

run show mvrp interface statistics

The **run show mvrp interface statistics** command is used to view the interface statistics information of MVRP packets on a specific interface.

Command Syntax

run show mvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- View the statistics information of MVRP.

```
admin@PICOS# run show mvrp interface te-1/1/21 statistics
packet_received: 245
packet_sent:     248
```

set protocols mvrp edge-switch

The **set protocols mvrp edge-switch** command can be used to enable or disable MVRP edge-switch function.

The **delete protocols mvrp edge-switch** command deletes the configuration.

> **NOTE:**
> This command can be enabled only on the edge switches.

Command Syntax

set protocols mvrp edge-switch <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP edge-switch function. The value could be **true** or **false**. • **true**: Enable MVRP edge-switch function. • **false**: Disable MVRP edge-switch function. By default, MVRP edge-switch function is disabled.

Example

- Enable MVRP edge-switch function.

```
admin@PICOS# set protocols mvrp edge-switch true
admin@PICOS# commit
```

set protocols mvrp enable

The **set protocols mvrp enable** command can be used to enable or disable MVRP function globally.

The **delete protocols mvrp enable** command deletes the configuration.

> **NOTE:**
> To enable MVRP function, users need to enable MVRP BOTH globally and at the per-interface level. The command **set protocols mvrp interface enable** enables MVRP function on a specific interface.

Command Syntax

set protocols mvrp enable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP function globally. The value could be **true** or **false**. • **true**: Enable MVRP function globally. • **false**: Disable MVRP function globally. By default, MVRP function is disabled.

Example

- Enable MVRP function globally.

```
admin@PICOS# set protocols mvrp enable true
admin@PICOS# commit
```

set protocols mvrp interface enable

The **set protocols mvrp interface enable** command can be used to enable or disable MVRP function on a specific interface.

The **delete protocols mvrp interface enable** command deletes the configuration.

> **NOTE:**
> To enable MVRP function, users need to enable MVRP BOTH globally and at the per-interface level. The command **set protocols mvrp enable** enables MVRP function globally.

Command Syntax

set protocols mvrp interface <*interface-name*> **enable** <**true | false**>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface or a LAG interface.
<**true	false**>	Enable or disable MVRP function on a specific interface. The value could be **true** or **false**. • **true**: Enable MVRP function on a specific interface. • **false**: Disable MVRP function on a specific interface. By default, MVRP function is disabled.

Example

- Enable MVRP function on a specific interface.

```
admin@PICOS# set protocols mvrp interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols mvrp traceoptions flag config

The **set protocols mvrp traceoptions flag config** command can be used to enable or disable MVRP debugging for configuration tracing.

The **delete protocols mvrp traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols mvrp traceoptions flag config disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable MVRP debugging for configuration tracing. • **false**: Enable MVRP debugging for configuration tracing. By default, MVRP debugging for configuration tracing is disabled.

Example

- Enable MVRP debugging for configuration tracing.

```
admin@PICOS# set protocols mvrp traceoptions flag config disable false
admin@PICOS# commit
```

set protocols mvrp traceoptions flag packets

The **set protocols mvrp traceoptions flag packets** command can be used to enable or disable MVRP debugging for received/sent packets event tracing.

The **delete protocols mvrp traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols mvrp traceoptions flag packets disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP debugging for received/sent packets event tracing. The value could be **true** or **false**. • **true**: Disable MVRP debugging for received/sent packets event tracing. • **false**: Enable MVRP debugging for received/sent packets event tracing. By default, MVRP debugging for received/sent packets event tracing is disabled.

Example

- Enable MVRP debugging for received/sent packets event tracing.

```
admin@PICOS# set protocols mvrp traceoptions flag packets disable false
admin@PICOS# commit
```

set protocols mvrp join-timer

The **set protocols mvrp join-timer** command configures the join timer duration for MVRP.

The **delete protocols mvrp join-timer** command deletes the configuration.

> **NOTE**s:
> It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp join-timer *<join-timer>*

delete protocols mvrp join-timer

Parameter

Parameter	Description
<join-timer>	Specifies the join timer. The value is an integer in milliseconds that ranges from 100 to 500. The default value is 200 milliseconds.

Example

- Configure the join timer.

```
admin@PICOS# set protocols mvrp join-timer 300
admin@PICOS# commit
```

set protocols mvrp leave-timer

The **set protocols mvrp leave-timer** command configures the leave timer duration for MVRP.

The **delete protocols mvrp leave-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp leave-timer *<leave-timer>*

delete protocols mvrp leave-timer

Parameter

Parameter	Description
<leave-timer>	Specifies the leave timer. The value is an integer in milliseconds that ranges from 300 to 1000. The default value is 1000 milliseconds.

Example

- Configure the leave timer.

```
admin@PICOS# set protocols mvrp leave-timer 800
admin@PICOS# commit
```

set protocols mvrp leaveall-timer

The **set protocols mvrp leaveall-timer** command configures the leaveall timer duration for MVRP.

The **delete protocols mvrp leaveall-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp leaveall-timer *<leaveall-timer>*

delete protocols mvrp leaveall-timer

Parameter

Parameter	Description
<leaveall-timer>	Specifies the leaveall timer. The value is an integer in seconds that ranges from 10 to 60. The default value is 10 seconds.

Example

- Configure the leaveall timer.

```
admin@PICOS# set protocols mvrp leaveall-timer 50
admin@PICOS# commit
```

ERPS Commands

- run show erps brief
- run show erps interface
- run show erps ring
- run show erps statistics
- set protocols erps ring
- set protocols erps version
- set protocols erps enable
- set protocols erps ring instance
- set protocols erps ring instance control-vlan
- set protocols erps ring instance description
- set protocols erps ring instance enable
- set protocols erps ring instance guard-timer
- set protocols erps ring instance holdoff-timer
- set protocols erps ring instance protected-instance
- set protocols erps ring instance r-aps level
- set protocols erps ring instance rpl
- set protocols erps ring instance wtr-timer
- set protocols erps ring port0 interface
- set protocols erps ring port1 interface
- set protocols erps ring r-aps ring-mac
- set protocols erps ring sub-ring
- set protocols erps ring virtual-channel
- set protocols erps ring instance non-revertive
- set protocols erps tcn-propagation
- set protocols erps ring instance connect ring
- erps switch force ring instance
- erps switch manual ring instance
- erps clear ring ring instance
- set protocols erps traceoptions flag all disable
- set protocols erps traceoptions flag config disable
- set protocols erps traceoptions flag ring disable

run show erps brief

The **run show erps brief** command shows brief information of the ERPS configuration.

Command Syntax

run show erps brief

Parameter

None.

Example

- View the brief information of the ERPS configuration.

```
admin@PICOS# run show erps brief
Enable: true
Version: 2
Tcn-propagation: Yes

D: Discarding
F: Forwarding
R: RPL Owner
N: RPL Neighbour
FS: Forced Switch
MS: Manual Switch
Ring ID    Instance ID    Control VLAN    Port0             Port1
--------------------------------------------------------------------------------
1          1              4001            te-1/1/19(D,R)    te-1/1/7(F)
2          2              4002            te-1/1/19(F)      te-1/1/7(F)
3          3              4003            te-1/1/19(F)      te-1/1/7(D,R)
```

run show erps interface

The **run show erps interface** command is used to view ERPS interface information, including Port Role, Port State and Signal Failure.

Command Syntax

run show erps interface ring <*ring-id*> **instance** <*instance-id*>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View ERPS interface information.

```
admin@PICOS# run show erps interface ring 1 instance 1
Interface      Port Role       Port State       Signal Failure
---------------------------------------------------------------
te-1/1/19      RPL Owner       Discarding       Non-failed
te-1/1/7       Common          Forwarding       Non-failed
```

run show erps ring

The **run show erps ring** command shows the detailed information of the ERPS ring instances.

Command Syntax

run show erps ring <*ring-id*> [**instance** <*instance-id*>]

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Optional. Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View the detailed information of the ERPS ring instances.

```
admin@PICOS# run show erps ring 1
Ring ID: 1
Port0: te-1/1/19
Port1: te-1/1/7
Ring-MAC: false
Sub-ring: No
Virtual-channel: No

Instance ID: 1
Enable: Yes
Active: true
Node state: Protection
Description:
Control VLAN: 4001
Protected instance: 1
Protected VLAN: 100-101,111,4094
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 1 min
Revertive mode: Revertive
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role        Port State       Signal Failure
-----------------------------------------------------------------
te-1/1/19      RPL Owner        Forwarding       Non-failed
te-1/1/7       Common           Forwarding       Non-failed


Instance ID: 2
Enable: Yes
Active: true
Node state: Protection
Description:
Control VLAN: 4002
Protected instance: 2
Protected VLAN: 200-201
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 1 min
Revertive mode: Revertive
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
```

```
Manual Switch Port: -
Interface      Port Role       Port State       Signal Failure
-------------------------------------------------------------------
te-1/1/19      Common          Forwarding       Non-failed
te-1/1/7       Common          Forwarding       Non-failed
```

In the show result,

- The parameter “**Active**” indicates whether the ERPS ring instance is active or not. If the configurations of the ERPS ring instance are correct and complete, the ERPS ring instance is active, and it shows “**Active: true**”.
- The parameter “**Node State**” indicates the state for the node:
  - **Init**: Not a participant of a specific ring.
  - **Idle**: No failure on the ring. Indicates that the current blocking point is at the RPL Owner port.
  - **Protection**: Indicates link failure or equipment fault on the ring.
  - **Pending**: Indicates a transition state for ERPS ring, such as the node is recovering from failure.
  - **Forced Switch**: Indicates that the ERPS ring port is blocked by forced switching.
  - **Manual Switch**: Indicates that the ERPS ring port is blocked by manual switching.

run show erps statistics

The **run show erps statistics** command shows the statistics of ERPS protocol messages sent and received by the ERPS ring ports.

Command Syntax

run show erps statistics [**ring** <*ring-id*> [**instance** <*instance-id*>]]

Parameter

Parameter	Description
ring <*ring-id*>	Optional. Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Optional. Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View the statistics information of ERPS packets.

```
admin@PICOS# run show erps statistics ring 7
Statistics for ERPS ring 7 instance 1:
R-APS       Port0 Tx     Port0 Rx     Port1 Tx     Port1 Rx
---------   ----------   ----------   ----------   ----------
NR          14           13           14           13
NR,RB       0            1393         0            1
SF          0            0            0            0
MS          0            0            0            0
FS          0            0            0            0
EVENT       6            3            6            9
```

In the show result,

- Rx: Indicates the receiving protocol messages.
- Tx: Indicates the sending protocol messages.
- NR: Indicates the statistics of R-APS (NR) messages.
- NR,RB: Indicates the statistics of R-APS (NR, RB) messages.
- SF: Indicates the statistics of R-APS (SF) messages.
- MS: Indicates the statistics of protocol messages of blocking the port by manual switching.
- FS: Indicates the statistics of protocol messages of blocking the port by forced switching.
- EVENT: Indicates the statistics of Event protocol messages.

set protocols erps ring

The **set protocols erps ring** command creates an ERPS ring with a given ID.

The **delete protocols erps ring** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*>

delete protocols erps ring <*ring-id*>

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.

Usage Guidelines

ERPS ring defined in command **set protocols erps ring** <*ring-id*> is a physical ring, however, ring instance can be thought as a logical ring on the physical ring defined in command **set protocols erps ring** <*ring-id*> **instance** <**1 | 2**>. A maximum of eight ERPS rings (including both major ring and sub-ring) are supported on a device, and a maximum of two instances can be configured for each ring.

Example

- Create an ERPS ring with a given ID.

```
admin@PICOS# set protocols erps ring 5
admin@PICOS# commit
```

set protocols erps version

The **set protocols erps version** command configures ERPS version, which could be ERPSv1 or ERPSv2.

The **delete protocols erps version** command restores the configuration to the default value ERPSv2.

Command Syntax

set protocols erps version <1 | 2>

delete protocols erps version

Parameters

Parameter	Description
version <1 | 2>	Specifies ERPS version. The default version is ERPSv2.

Usage Guidelines

PICOS supports both versions of ERPSv1 and ERPSv2. ERPSv2 is fully compatible with ERPSv1 and has the following extensions:

- Sub-ring supporting
- Sub-ring virtual channel/non-virtual channel transmission of RAPS messages
- Manual switching of port blocking, including Forced Switch and Manual Switch
- ERPS ring revertive/non-revertive modes are configurable
- Sub-ring topology change notifications

ERPSv1 only supports major ring networking, while ERPSv2 supports not only major ring, but also supports sub-ring network, and the mixed networking of major ring and sub-ring.

Example

- Configure the ERPS version.

```
admin@PICOS# set protocols erps version 1
admin@PICOS# commit
```

set protocols erps enable

The **set protocols erps enable** command can be used to enable or disable ERPS function globally.

The **delete protocols erps enable** command deletes the configuration.

Command Syntax

set protocols erps enable <**true | false**>

delete protocols erps enable

Parameters

Parameter	Description
<**true	false**>	Enable or disable ERPS function globally. The value could be **true** or **false**. • **true**: Enable ERPS function globally. • **false**: Disable ERPS function globally. By default, ERPS function is disabled.

Example

- Enable ERPS function globally.

```
admin@PICOS# set protocols erps enable true
admin@PICOS# commit
```

set protocols erps ring instance

The **set protocols erps ring instance** command creates an instance for the ERPS ring.

The **delete protocols erps ring instance** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <**1 | 2**>

delete protocols erps ring <*ring-id*> **instance**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <**1	2**>	Specifies the instance ID for a ring. The value is an integer that could be 1 or 2.

Usage Guidelines

ERPS ring defined in command **set protocols erps ring** <*ring-id*> is a physical ring, however, ring instance can be thought as a logical ring on the physical ring defined in command **set protocols erps ring** <*ring-id*> **instance** <**1 | 2**>. A maximum of eight ERPS rings are supported on a device, and a maximum of two instances can be configured for each ring.

Example

- Create an ERPS ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2
admin@PICOS# commit
```

set protocols erps ring instance control-vlan

The **set protocols erps ring instance control-vlan** command adds a control VLAN to a ring instance.

The **delete protocols erps ring instance control-vlan** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **control-vlan** <*control-vlan*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **control-vlan**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
control-vlan <*control-vlan*>	Specifies the control VLAN ID for a ring instance. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In an ERPS ring, the control VLAN is used to transmit ERPS protocol packets.

- Each ERPS ring instance must be configured with a control VLAN.
- Different ERPS ring instances cannot use the same control VLAN.
- The same control VLAN must be configured for all devices in the same ERPS ring instance.

Example

- Add a control VLAN to a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 control-vlan 100
admin@PICOS# commit
```

set protocols erps ring instance description

The **set protocols erps ring instance description** command configures the descriptive information to help administrators and operators understand the purpose of a ring instance.

The **delete protocols erps ring instance description** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **description** <*text*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **description**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
description <*text*>	Specifies the descriptive information about the ring instance. The value is a string.

Example

- Configure the descriptive information about the ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 description WestInstance
admin@PICOS# commit
```

set protocols erps ring instance enable

The **set protocols erps ring instance enable** command can be used to enable or disable protection switching on the given instance of the ring. It is disabled by default.

The **delete protocols erps ring instance enable** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **enable** <**true | false**>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **enable**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
enable <**true	false**>	Enable or disable protection switching on the given instance of the ring. The value could be **true** or **false**. • **true**: Enable protection switching on the given instance of the ring. • **false**: Disable protection switching on the given instance of the ring. By default, ERPS ring instance is disabled.

Usage Guidelines

ERPS ring instance can be enabled by the command **set protocols erps ring** <*ring-id*> **instance** <*instance-id*> **enable true**, or by configuring other "**set protocols erps ring** <*ring-id*> **instance** <*instance-id*> xxx" commands in the ERPS CLI.

The command **set protocols erps ring** <*ring-id*> **instance** <*instance-id*> **enable false** can be used to disable ERPS ring instance on the device.

Example

- Enable protection switching on the given instance of the ring.

```
admin@PICOS# set protocols erps ring 5 instance 2 enable true
admin@PICOS# commit
```

set protocols erps ring instance guard-timer

The **set protocols erps ring instance guard-timer** command configures the guard timer duration for a ring instance.

The **delete protocols erps ring instance guard-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **guard-timer** <*guard-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **guard-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
guard-timer <*guard-timer*>	Specifies the guard timer duration of a ring instance. The value is an integer, in milliseconds, that ranges from 10 to 2000. The default value is 500 milliseconds.

Example

- Configure the guard timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 guard-timer 300
admin@PICOS# commit
```

set protocols erps ring instance holdoff-timer

The **set protocols erps ring instance holdoff-timer** command configures the holdoff timer for a ring instance.

The **delete protocols erps ring instance holdoff-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **holdoff-timer** <*holdoff-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **holdoff-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
holdoff-timer <*holdoff-timer*>	Specifies the holdoff timer of a ring instance. The value is an integer, in milliseconds, that ranges from 0 to 10000. The default value is 0 millisecond.

Example

- Configure the holdoff timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 holdoff-timer 1000
admin@PICOS# commit
```

set protocols erps ring instance protected-instance

The **set protocols erps ring instance protected-instance** command configures the MSTP instance of VLANs that is protected by the ring instance.

The **delete protocols erps ring instance protected-instance** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **protected-instance** <*msti*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **protected-instance**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
protected-instance <*msti*>	Specifies the MSTP instance of VLANs that are protected by this ring instance. The value is an integer that ranges from 1 to 16.

Usage Guidelines

protected-instance <*msti*> is the MSTP instance that are protected by the ring instance, so MSTP instance and VLAN mapping needs to be configured before configure ERPS by using command: **set protocols spanning-tree mstp msti** <*msti*> **vlan** <*vlan-id*>.

Make sure that the control VLAN and data VLANs of the ERPS ring have all been mapped to the MSTP instance.

The traffic of MSTP instance 0 is blocked by ERPS ring.

Multiple protected-instance (protected MSTP instance) can be added to one ERPS instance.

Example

- Configure the MSTP instance that is protected by this ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 protected-instance 6
admin@PICOS# commit
```

set protocols erps ring instance r-aps level

The **set protocols erps ring instance r-aps level** command configures the Automatic Protection Switching (APS) message level for the node on the ERPS ring.

The **delete protocols erps ring instance r-aps level** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **r-aps level** <*level-id*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **r-aps level**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
level <*level-id*>	Specifies the Automatic Protection Switching (APS) message level for the node on the Ethernet ring. The value is an integer that ranges from 1 to 7. The default value of r-aps level is 7.

Usage Guidelines

The default value of r-aps level is 7. All nodes in the ethernet ring must be configured with the same level.

Each ERPS node can only process APS messages with an r-aps level value less than or equal to itself. If a ring port receives an APS message with an R-APS level value larger than its own, all the ring ports belonging to this ERPS instance will become blocking.

Example

- Configure the Automatic Protection Switching (APS) message level for the node.

```
admin@PICOS# set protocols erps ring 5 instance 2 r-aps level 5
admin@PICOS# commit
```

set protocols erps ring instance rpl

The **set protocols erps ring instance rpl** command configures RPL port role for the ERPS ring instance.

The **delete protocols erps ring instance rpl** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **rpl** <**port0** | **port1**> <**owner** | **neighbor**>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **rpl** [<**port0** | **port1**>]

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
<port0 | port1>	Specifies ERPS ring **port0** or **port1**.
<**owner** | **neighbor**>	Specifies RPL port role for the ERPS ring instance. The value could be **owner** or **neighbor**. • **owner**: RPL owner port. • **neighbor**: RPL neighbor port. ERPS ports are ordinary ports if no RPL port role is designated.

Usage Guidelines

Each ERPS ring instance has only one RPL owner port and neighbor port, which are determined by user configuration. By blocking the RPL owner port and neighbor port to forward user traffic, it prevents network loops in the ERPS ring.

Example

- Configure port0 as the RPL owner port for the ERPS ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 rpl port0 owner
admin@PICOS# commit
```

set protocols erps ring instance wtr-timer

The **set protocols erps ring instance wtr-timer** command configures the WTR timer for a ring instance.

The **delete protocols erps ring instance wtr-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **wtr-timer** <*wtr-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **wtr-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
wtr-timer <*wtr-timer*>	Specifies the WTR timer duration of a ring instance. The value is an integer, in minutes, that ranges from 1 to 12. The default value is 5 minutes.

Example

- Configure the WTR timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 wtr-timer 5
admin@PICOS# commit
```

set protocols erps ring port0 interface

The **set protocols erps ring port0 interface** command configures port0 of an ERPS ring. An L2 interface in the switch is associated to one of the two member ports (port0 and port1) of an ERPS ring. No more than two ports per node can join the same ERPS ring, which are named ERPS **port0** and **port1**.

The **delete protocols erps ring port0 interface** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **port0 interface** <*interface-name*>

delete protocols erps ring <*ring-id*> **port0 interface**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies port0 interface name of ERPS ring. The value is a physical port.

Example

- Configure port0 of an ERPS ring.

```
admin@PICOS# set protocols erps ring 5 port0 interface ge-1/1/1
admin@PICOS# commit
```

set protocols erps ring port1 interface

The **set protocols erps ring port1 interface** command configures port1 of an ERPS ring. An L2 interface in the switch is associated to one of the two member ports (port0 and port1) of an ERPS ring. No more than two ports per node can join the same ERPS ring, which are named ERPS **port0** and **port1**.

The **delete protocols erps ring port1 interface** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **port1 interface** <*interface-name*>

delete protocols erps ring <*ring-id*> **port1 interface**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies port1 interface name of ERPS ring. The value is a physical port.

Example

- Configure port1 of an ERPS ring.

```
admin@PICOS# set protocols erps ring 5 port1 interface ge-1/1/2
admin@PICOS# commit
```

set protocols erps ring r-aps ring-mac

The **set protocols erps ring r-aps ring-mac** command configure the ring ID as the last byte of the destination MAC address for R-APS packets.

The **delete protocols erps ring r-aps ring-mac** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **r-aps ring-mac**

delete protocols erps ring <*ring-id*> **r-aps ring-mac**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.

Example

- Configure the ERPS ring ID 5 as the last byte of the destination MAC address for R-APS packets.

```
admin@PICOS# set protocols erps ring 5 r-aps ring-mac
admin@PICOS# commit
```

set protocols erps ring sub-ring

The **set protocols erps ring sub-ring** command configures a sub-ring. If not specified, the ring is a major ring.

The **delete protocols erps ring sub-ring** command removes the sub-ring configuration of the ring and sets it to be a major ring. Other sub-ring configurations, such as tcn-propagation function, will no longer take effect.

Command Syntax

set protocols erps ring <*ring-id*> **sub-ring** <**true | false**>

delete protocols erps ring<*ring-id*>**sub-ring**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
<**true	false**>	Enable or disable ERPS sub-ring. The value could be **true** or **false**. • **true**: Enable ERPS sub-ring. • **false**: Disable ERPS sub-ring. By default, the ERPS ring is a major ring.

Example

- Configure a sub-ring.

```
admin@PICOS# set protocols erps ring 5 sub-ring true
admin@PICOS# commit
```

set protocols erps ring virtual-channel

The **set protocols erps ring virtual-channel** command enables virtual-channel RAPS message transmission method for a sub-ring. By default, the sub-ring RAPS message is transmitted as a non-virtual channel.

The **delete protocols erps ring virtual-channel** command restores the configuration to the default value.

Command Syntax

set protocols erps ring <*ring-id*> **virtual-channel** <**true | false**>

delete protocols erps ring <*ring-id*> **virtual-channel**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
<**true	false**>	Enable or disable virtual-channel sub-ring RAPS message transmission method. The value could be **true** or **false**. • **true**: Enable virtual-channel sub-ring RAPS message transmission method. • **false**: Disable virtual-channel sub-ring RAPS message transmission method. By default, the sub-ring RAPS message is transmitted as a non-virtual channel.

Usage Guidelines

To enable Virtual-Channel method, the following configurations are required:

1. Enable virtual channel on all the devices of the sub-ring, where the <*ring-id*> is the sub-ring ID.

   set protocols erps ring <*ring-id*> **virtual-channel** <**true | false**>

2. Add the major ring port, which is used for forwarding R-APS messages from the sub-ring, to the control VLAN of the sub-ring.

Example

- Enable virtual-channel RAPS message transmission method for sub-ring 5.

```
admin@PICOS# set protocols erps ring 5 virtual-channel true
admin@PICOS# commit
```

set protocols erps ring instance non-revertive

The **set protocols erps ring instance non-revertive** command configures ERPS non-revertive mode. By default, the ERPS ring is in revertive mode.

The **delete protocols erps ring instance non-revertive** command restores the configuration to the default value, that is, the revertive mode.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **non-revertive** <**true | false**>

delete protocols erps ring<*ring-id*>**instance** <*instance-id*> **non-revertive**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
<**true	false**>	Enable or disable ERPS non-revertive mode. The value could be **true** or **false**. • **true**: Enable ERPS non-revertive mode. • **false**: Disable ERPS non-revertive mode. By default, ERPS works at revertive mode.

Example

- Configure ERPS non-revertive mode.

```
admin@PICOS# set protocols erps ring 5 instance 2 non-revertive true
admin@PICOS# commit
```

set protocols erps tcn-propagation

The **set protocols erps tcn-propagation** command enables sub-ring topology change notifications. When the topology of the sub-ring changes, the FDB refresh of the port will generate a Topology Change (TC) signal. When the tcn-propagation function is enabled, the intersecting node sends an event flush message to the connect ring when it receives the TC signal.

The **delete protocols erps tcn-propagation** command disables sub-ring topology change notifications.

Command Syntax

set protocols erps tcn-propagation <**true | false**>

delete protocols erps tcn-propagation

Parameter

Parameter	Description
<**true	false**>	Enable or disable topology change notifications. The value could be **true** or **false**. • **true**: Enable sub-ring topology change notifications. • **false**: Disable sub-ring topology change notifications. By default, sub-ring topology change notifications is disabled.

Usage Guidelines

To enable sub-ring topology change notifications, the following configurations are required:

1. Configure the connect ring for a sub-ring on all intersecting nodes.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **connect ring** <*ring-id*> **instance** <*instance-id*>

2. Enable tcn-propagation function to advertise topology changes to the connect ring on all intersecting nodes.

set protocols erps tcn-propagation <**true | false**>

Example

- Enable sub-ring topology change notifications.

```
admin@PICOS# set protocols erps tcn-propagation true
admin@PICOS# commit
```

set protocols erps ring instance connect ring

The **set protocols erps ring instance connect ring** command configures the connect ring for a sub-ring. Associate a ring with a sub-ring if you want to advertise topology changes in a sub-ring to a ring.

The **delete protocols erps ring instanceconnect ring** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id1*> **instance** <*instance-id1*> **connect ring** <*ring-id2*> **instance** <*instance-id2*>

delete protocols erps ring <*ring-id1*> **instance** <*instance-id1*> **connect ring** <*ring-id2*> **instance** <*instance-id2*>

Parameter

Parameter	Description
ring <*ring-id1*>	Specifies the ID of the local sub-ring ID. The value is an integer that ranges from 1 to 8.
instance <*instance-id1*>	Specifies the instance ID for a local sub-ring. The value is an integer that ranges from 1 to 2.
ring <*ring-id2*>	Specifies the ID of the connect ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id2*>	Specifies the instance ID for the connect ring. The value is an integer that ranges from 1 to 2.

Example

- Configure the connect ring 6 for sub-ring 5.

```
admin@PICOS# set protocols erps ring 5 instance 2 connect ring 6 instance 1
admin@PICOS# commit
```

erps switch force ring instance

The **erps switch force ring instance** command configures to block a specific ring instance in the way of force switch in CLI operational mode.

Command Syntax

erps switch force ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps switch force ring** <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

ERPS supports two switching methods to manually configure port blocking:

- **Forced switch**: Ports configured for forced switch are blocked immediately, regardless of whether other links on the ring are faulty or not.
- **Manual switch**: Ports configured for manual switch are blocked if the state of the ring is Idle or Pending, otherwise they are not blocked.

The **run show erps ring** command can be used to show the node state of the ERPS ring instances. If force switch (or manual switch) is set successfully, the ***Node state*** in the show result displays **Forced Switch** (or **Manual Switch**).

The **erps clear ring instance** command can be used to clear the blocking point switching operation of the ERPS ring.

Example

- Configure to block a specific ring instance in the way of force switch.

```
admin@PICOS> erps switch force ring 5 instance 2 port0
```

erps switch manual ring instance

The **erps switch manual ring instance** command configures to block a specific ring instance in the way of manual switch in CLI operational mode.

Command Syntax

erps switch manual ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps switch manual ring** <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

ERPS supports two switching methods to manually configure port blocking:

- **Forced switch**: Ports configured for forced switch are blocked immediately, regardless of whether other links on the ring are faulty or not.
- **Manual switch**: Ports configured for manual switch are blocked if the state of the ring is Idle or Pending, otherwise they are not blocked.

The **run show erps ring** command can be used to show the node state of the ERPS ring instances. If force switch (or manual switch) is set successfully, the ***Node state*** in the show result displays **Forced Switch** (or **Manual Switch**).

The **erps clear ring instance** command can be used to clear the blocking point switching operation of the ERPS ring.

Example

- Configure to block a specific ring instance in the way of manual switch.

```
admin@PICOS> erps switch manual ring 6 instance 1 port1
```

erps clear ring ring instance

The **erps clear ring instance** command is used to clear the blocking point switching operation of the ERPS ring in CLI operational mode.

Command Syntax

erps clear ring <*ring-id*> **instance** <*instance-id*>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps clear ring ring** <*ring-id*> **instance** <*instance-id*> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

Clear operation is used in the following three cases:

- Clearing the locally configured manual switch and forced switch configurations.
- When the ERPS ring is in the revertive mode, the revert action is triggered manually before the WTB Timer/WTR Timer times out.
- When the ERPS ring is in non-revertive mode, the revert action is triggered manually.

Example

- Configure to clear the blocking point switching operation.

```
admin@PICOS> erps clear ring 6 instance 1
```

set protocols erps traceoptions flag all disable

The **set protocols erps traceoptions flag all disable** command can be used to enable or disable ERPS debugging for tracing all ERPS operations.

The **delete protocols erps traceoptions flag all disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag all disable <**true | false**>

delete protocols erps traceoptions flag all disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for tracing all ERPS operations. The value could be **true** or **false**. • **true**: Disable ERPS debugging for tracing all ERPS operations. • **false**: Enable ERPS debugging for tracing all ERPS operations. By default, ERPS debugging for tracing all ERPS operations is disabled.

Example

- Enable ERPS debugging for tracing all ERPS operations.

```
admin@PICOS# set protocols erps traceoptions flag all disable false
admin@PICOS# commit
```

set protocols erps traceoptions flag config disable

The **set protocols erps traceoptions flag config disable** command can be used to enable or disable ERPS debugging for configuration tracing.

The **delete protocols erps traceoptions flag config disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag config disable <**true | false**>

delete protocols erps traceoptions flag config disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable ERPS debugging for configuration tracing. • **false**: Enable ERPS debugging for configuration tracing. By default, ERPS debugging for configuration tracing is disabled.

Example

- Enable ERPS debugging for configuration tracing.

```
admin@PICOS# set protocols erps traceoptions flag config disable false
admin@PICOS# commit
```

set protocols erps traceoptions flag ring disable

The **set protocols erps traceoptions flag ring disable** command can be used to enable or disable ERPS debugging for all the ERPS tracing except the configuration operation.

The **delete protocols erps traceoptions flag ring disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag ring disable <**true | false**>

delete protocols erps traceoptions flag ring disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for all the ERPS tracing except the configuration operation. The value could be **true** or **false**. • **true**: Disable ERPS debugging for all the ERPS tracing except the configuration operation. • **false**: Enable ERPS debugging for all the ERPS tracing except the configuration operation. By default, ERPS debugging for all the ERPS tracing except the configuration operation is disabled.

Example

- Enable ERPS debugging for all the ERPS tracing except the configuration operation.

```
admin@PICOS# set protocols erps traceoptions flag ring disable false
admin@PICOS# commit
```

EFM OAM Commands

- set protocols ethernet-oam interface enable
- set protocols ethernet-oam interface mode
- set protocols ethernet-oam interface remote-loopback supported
- set protocols ethernet-oam interface remote-loopback timeout
- ethernet-oam remote-loopback start|stop interface
- set protocols ethernet-oam interface timeout
- set protocols ethernet-oam traceoptions flag packets
- set protocols ethernet-oam traceoptions flag config
- run show ethernet-oam
- run show ethernet-oam statistics

set protocols ethernet-oam interface enable

The **set protocols ethernet-oam interface enable** command can be used to enable or disable EFM OAM function on a specific interface. Note that both ends of the connected OAM link need to be configured with this command to enable the EFM OAM function.

The **delete protocols ethernet-oam interface enable** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **enable** <**true | false**>

delete protocols ethernet-oam interface <*interface-name*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
<**true	false**>	Enable or disable EFM OAM function on a specific interface. The value could be **true** or **false**. • **true**: Enable EFM OAM function on a specific interface. • **false**: Disable EFM OAM function on a specific interface. By default, EFM OAM function is disabled.

Example

- Enable EFM OAM function on a specific interface.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols ethernet-oam interface mode

The **set protocols ethernet-oam interface mode** command configures the EFM OAM mode for the Ethernet port enabled EFM OAM function.

The **delete protocols ethernet-oam interface mode** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **mode** <**active | passive**>

delete protocols ethernet-oam interface <*interface-name*> **mode**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
mode <**active	passive**>	Specifies the EFM OAM mode. The value could be **active** or **passive**. • **Active** mode causes the port to initiate the negotiation process and continually send out EFM OAM information PDUs. • **Passive** mode waits for the peer to initiate the negotiation process. A passive mode port cannot initiate remote loopback activity with the peer. By default, the EFM OAM mode is **active**.

Example

- Configure the EFM OAM mode to **passive** for the Ethernet port enabled EFM OAM.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 mode passive
admin@PICOS# commit
```

set protocols ethernet-oam interface remote-loopback supported

The **set protocols ethernet-oam interface remote-loopback supported** command enables reactions to loopback control OAMPDUs from peers.

The **delete protocols ethernet-oam interface remote-loopback supported** command deletes the configuration.

> **NOTE**:
>
> The responding end has been configured with this command to enable reactions to loopback control OAMPDUs from peers, only after this can the peer end run the command **ethernet-oam remote-loopback start interface** <*interface-name*> to start the EFM OAM remote loopback tests.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **remote-loopback supported**

delete protocols ethernet-oam interface <*interface-name*> **remote-loopback supported**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface, for example, ge-1/1/1, xe-1/1/2, and so on.

Example

- Enable reactions to loopback control OAMPDUs from peers.

```
admin@PICOS# set protocols ethernet-oam interface xe-1/1/2 remote-loopback supported
admin@PICOS# commit
```

set protocols ethernet-oam interface remote-loopback timeout

The **set protocols ethernet-oam interface remote-loopback timeout** command configures the timeout for receiving remote loopback responding message. When times out, the EFM session state falls back to the DISCOVERY phase.

The **delete protocols ethernet-oam interface remote-loopback timeout** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **remote-loopback timeout** <*loopback-timeout*>

delete protocols ethernet-oam interface <*interface-name*> **remote-loopback timeout**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
timeout <*loopback-timeout*>	Specifies the timeout for remote loopback. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 3 seconds.

Example

- Configure the timeout for remote loopback.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 remote-loopback timeout 9
admin@PICOS# commit
```

ethernet-oam remote-loopback start|stop interface

The **ethernet-oam remote-loopback start interface** command starts EFM OAM remote loopback tests on the specific port. The EFM OAM remote loopback control OAMPDU will be sent to the peering device to trigger a remote loopback.

The **ethernet-oam remote-loopback stop interface** command stops EFM OAM remote loopback tests on the specific port. The EFM OAM remote loopback control OAMPDU will be sent to the peering device to stop a remote loopback.The **set protocols dot1x interface authentication-open disable** command enables

Command Syntax

ethernet-oam remote-loopback start interface <*interface-name*>

ethernet-oam remote-loopback stop interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface, for example, ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When configuring this command, pay attention to the following notes:

- The commands **ethernet-oam remote-loopback start interface** and **ethernet-oam remote-loopback stop interface** are operational mode commands which should be executed under the prompt “admin@PICOS>”.
- Only the **active** mode end can run these two commands to start or stop EFM OAM remote loopback tests.
- Before starting the EFM OAM remote loopback tests, make sure:
  - The EFM OAM connection has been established successfully.
  - Users have to configure command **set protocols ethernet-oam interface** <*interface-name*> **remote-loopback supported** on the responding end to enable reactions to loopback control OAMPDUs from peers.
- EFM OAM remote loopback tests will fail if above conditions are not met. After all of the conditions are met, you need to execute the command **ethernet-oam remote-loopback start interface** <*interface-name*> again to start EFM OAM remote loopback tests again.
- When remote loopback function is implemented, the interface no longer participates in any other Layer 2 or Layer 3 protocols.
- When the remote loopback test is completed, you should use the command **ethernet-oam remote-loopback stop interface** to disable EFM OAM remote loopback tests on the port.
- It is not allowed to modify the EFM OAM mode when remote loopback function is implementing.
- The device sends a Loopback Control OAMPDU to the peer when run command **ethernet-oam remote-loopback start interface** <*interface-name*> or **ethernet-oam remote-loopback stop interface** <*interface-name*>.

Example

- Start EFM OAM remote loopback tests on the specific port.

```
admin@PICOS> ethernet-oam remote-loopback start interface te-1/1/1
```

- Stop EFM OAM remote loopback tests on the specific port.

```
admin@PICOS> ethernet-oam remote-loopback stop interface te-1/1/1
```

set protocols ethernet-oam interface timeout

The **set protocols ethernet-oam interface timeout** command configures the timeout for receiving the EFM OAM protocol messages. When the timeout timer expires, the local OAM entity ages out and terminates its connection with the peer OAM entity.

The **delete protocols ethernet-oam interface timeout** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **timeout** <*oam-timeout*>

delete protocols ethernet-oam interface <*interface-name*> **timeout**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
timeout <*oam-timeout*>	Specifies the timeout for receiving EFM protocol messages. The value is an integer, in seconds, that ranges from 2 to 30. The default value is 5 seconds.

Example

- Configure the timeout for receiving EFM protocol messages.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 timeout 10
admin@PICOS# commit
```

set protocols ethernet-oam traceoptions flag packets

The **set protocols ethernet-oam traceoptions flag packets** command can be used to enable or disable EFM OAM debugging for received/sent packets tracing.

The **delete protocols ethernet-oam traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols ethernet-oam traceoptions flag packets disable <**true | false**>

delete protocols ethernet-oam traceoptions flag packets

Parameter

Parameter	Description
<**true	false**>	Enable or disable EFM OAM debugging for received/sent packets tracing. The value could be **true** or **false**. • **true**: Disable EFM OAM debugging for received/sent packets tracing. • **false**: Enable EFM OAM debugging for received/sent packets tracing. By default, EFM OAM debugging for received/sent packets tracing is disabled.

Example

- Enable EFM OAM debugging for received/sent packets tracing.

```
admin@PICOS# set protocols ethernet-oam traceoptions flag packets disable false
admin@PICOS# commit
```

set protocols ethernet-oam traceoptions flag config

The **set protocols ethernet-oam traceoptions flag config** command can be used to enable or disable EFM OAM debugging for configuration tracing.

The **delete protocols ethernet-oam traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols ethernet-oam traceoptions flag config disable <**true | false**>

delete protocols ethernet-oam traceoptions flag config

Parameter

Parameter	Description
<**true	false**>	Enable or disable EFM OAM debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable EFM OAM debugging for configuration tracing. • **false**: Enable EFM OAM debugging for configuration tracing. By default, EFM OAM debugging for configuration tracing is disabled.

Example

- Enable EFM OAM debugging for configuration tracing.

```
admin@PICOS# set protocols ethernet-oam traceoptions flag config disable false
admin@PICOS# commit
```

run show ethernet-oam

The **run show ethernet-oam** command is used to view EFM OAM information and session status.

Command Syntax

run show ethernet-oam [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled EFM OAM. The value is a physical interface. If not specified, EFM OAM information and session status of all the interfaces enabled EFM OAM will be displayed.

Example

- View EFM OAM information and session status.

```
admin@PICOS# run show ethernet-oam interface ge-1/1/1
-------------------------------------------------
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          passive
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   local loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:5c:8c:21
    OUI:               48:6e:73
    PDU revision:       3
    OAM Mode:          active
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
Mtu size:          1500
```

The following table provides the description of the EFM OAM status information in the **run show ethernet-oam command** output.

Item	Description
Admin state	Whether the OAM function of an interface is enabled.

Loopback status	Indicates the status of remote loopback. The value could be **no loopback**, **remote loopback** or **local loopback**. • no loopback: Indicates that a remote loopback has not been established yet. • remote loopback: Indicates that a remote loopback has been established, and the device is the controlling end of the remote loopback, which starts EFM OAM remote loopback tests. • local loopback: Indicates that a remote loopback has been established, and the device is the controlled end of the remote loopback, which responds to the loopback control OAMPDUs from peers.
OAM status	Indicates the OAM status of an interface. The values are as follows: • PASSIVE_WAIT: indicates that the interface is waiting for protocol packets from the peer interface. • ACTIVE_SEND_LOCAL: indicates that the interface is sending protocol packets but fails to negotiate the link status with the peer interface. • ACTIVE_SEND_REMOTE_OK: indicates that the peer interface supports OAM and the negotiation with the peer interface is about to succeed. • SEND_ANY: indicates that the interface successfully negotiates the link status with the peer interface. • FAULT: indicates that the interface is abnormal and fails to establish an OAM connection.
PDU	The way in which the local end processes Ethernet OAMPDUs: • RX_INFO: The interface receives only Information OAMPDUs and does not send any Ethernet OAMPDUs. • LF_INFO: The interface sends only Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • INFO: The interface sends and receives only Information OAMPDUs. • ANY: The interface sends and receives Ethernet OAMPDUs of any type.

run show ethernet-oam statistics

The **run show ethernet-oam statistics** command is used to view the interface statistics information of EFM OAMPDU packets.

Command Syntax

run show ethernet-oam statistics [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled EFM OAM. The value is a physical interface. If not specified, statistics information of all the interfaces enabled EFM OAM will be displayed.

Example

- View the statistics information of EFM OAMPDU packets.

```
admin@PICOS# run show ethernet-oam statistics interface ge-1/1/1
Packets statistics for interface ge-1/1/1
Packet type                      OAM Tx Count     OAM Rx Count
-------------------------------------------------------------------------------
OAMInformation                  11365            11372
OAMLoopbackControl              0                1
OAMUnsupported                  0                0
```

MPLS Commands

- set protocols mpls interface
- set protocols mpls ldp router-id
- set protocols mpls ldp ordered-control
- set protocols mpls ldp neighbor password
- set protocols mpls ldp neighbor session-holdtime
- set protocols mpls ldp neighbor ttl-security disable
- set protocols mpls ldp neighbor ttl-security hops
- set protocols mpls ldp interface
- set protocols mpls ldp ttl-security disable (IP family)
- set protocols mpls ldp label-local-advertise
- set protocols mpls ldp label-local-allocate
- set protocols mpls ldp discovery transport-address
- set protocols mpls ldp discovery hello-interval
- set protocols mpls ldp discovery hello-holdtime
- set protocols mpls ldp discovery targeted-hello-interval
- set protocols mpls ldp discovery targeted-hello-holdtime
- set protocols mpls ldp discovery targeted-hello-accept
- set protocols mpls ldp dual-stack transport-connection prefer-ipv4
- set protocols mpls ldp dual-stack interop
- set protocols mpls ldp targeted-neighbor
- set protocols mpls ldp traceoption labels
- set protocols mpls ldp traceoption errors
- set protocols mpls ldp traceoption event
- set protocols mpls ldp traceoption discovery
- set protocols mpls ldp traceoption messages
- run show mpls ldp binding
- run show mpls ldp neighbor
- run show mpls ldp interface
- run show mpls forward-table
- run show mpls egress interface
- run show mpls table
- run show mpls interface
- run show mpls status
- run show mpls label
- run show mpls ldp discovery
- run show mpls fec

set protocols mpls interface

The **set protocols mpls interface** command enables MPLS on an L3 interface. Usually, both the incoming and outgoing interfaces of the packets need to enable MPLS.

The **delete protocols mpls interface** command deletes the configuration.

Command Syntax

set protocols mpls interface <*interface-name*> [**dummy**]

delete protocols mpls interface

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface to enable MPLS. The value could be a VLAN interface, loopback interface name, routed interface or sub-interface. By default, MPLS is disabled on all the interfaces.

Example

- Enable MPLS on interface vlan200.

```
admin@PICOS# set protocols mpls interface vlan200
admin@PICOS# commit
```

set protocols mpls ldp router-id

The **set protocols mpls ldp router-id** command configures a Router ID for the switch.

The **delete protocols mpls ldp router-id** command deletes the configuration.

Command Syntax

set protocols mpls ldp router-id *<router-id>*

delete protocols mpls ldp router-id

Parameter

Parameter	Description
router-id *<router-id>*	Specifies a Router ID. It is an IPv4 address in the A.B.C.D dotted decimal format (e.g., 192.0.2.1).

Usage Guidelines

MPLS LDP router ID is a crucial identifier for routers within an MPLS network. It is used to establish and maintain LDP sessions between routers. LDP sessions are responsible for the exchange of label binding information necessary for MPLS forwarding.

The Router ID must be unique within the MPLS network to avoid routing loops and ensure proper label distribution.

Using a loopback interface for the LDP Router ID is a best practice because loopback addresses are not tied to any physical interface and remain up as long as the router is operational, providing a stable identifier for LDP sessions.

Example

- Configure a Router ID for the switch.

```
admin@PICOS# set protocols mpls ldp router-id 2.2.2.2
admin@PICOS# commit
```

set protocols mpls ldp ordered-control

The **set protocols mpls ldp ordered-control** command configures LDP Ordered Label Distribution Control.

The **delete protocols mpls ldp ordered-control** command deletes the configuration.

Command Syntax

set protocols mpls ldp ordered-control

delete protocols mpls ldp ordered-control

Parameter

None.

Usage Guidelines

There are two ways of label distribution: **Ordered Control** and **Independent Control**.

- **Ordered Control**: The LSR has to receive the label mapping message of the next hop of the FEC, or when this LSR is the outgoing node of this FEC, it will assign labels to the FEC itself.
- **Independent Control**: LSR can autonomously assign labels to FEC without waiting for label mapping from downstream.

The default way is **Independent Control**.

Example

- Configure LDP Ordered Label Distribution Control.

```
admin@PICOS# set protocols mpls ldp ordered-control
admin@PICOS# commit
```

set protocols mpls ldp neighbor password

The **set protocols mpls ldp neighbor password** command enables message digest5 (MD5) authentication on a TCP connection between two MPLS LDP neighbors.

The **delete protocols mpls ldp neighbor password** command disables this feature.

Command Syntax

set protocols mpls ldp neighbor <*ip*> **password** <*text-password*>

delete protocols mpls ldp neighbor <*ip*> **password**

Parameter

Parameter	Description
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
password <*text-password*>	Specifies the txt password. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Usage Guidelines
By setting a password, you enforce authentication for the LDP session between the local router and its neighbor. This adds a layer of security, ensuring that only authorized routers can establish an LDP session and exchange label information.
It helps to prevent unauthorized devices from establishing LDP sessions with your routers, which could potentially lead to routing issues or security vulnerabilities.

NOTE:
Ensure that the same password is configured on both sides of the LDP session. Mismatched passwords will prevent the LDP session from being established.

Example
• This example enables message digest5 (MD5) authentication on a TCP connection between two MPLS LDP neighbors.

```
admin@XorPlus# set protocols mpls ldp neighbor 2.2.2.2 password picos12345
admin@XorPlus# commit
```

set protocols mpls ldp neighbor session-holdtime

The **set protocols mpls ldp neighbor session-holdtime** command configures the hold time period for keepalive. After this time of non response, the LDP established session will be considered as set to down.

The **delete protocols mpls ldp neighbor session-holdtime** command deletes the configuration.

Command Syntax

set protocols mpls ldp neighbor <*ip*> **session-holdtime**<*holdtime*>

delete protocols mpls ldp neighbor <*ip*> **session-holdtime**

Parameter

Parameter	Description
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a LDP peer.
session-holdtime <*holdtime*>	Specifies the hold time for keepalive. That value is an integer which can be configured between 15 and 65535 seconds. The default session hold time is 180 seconds.

Usage Guidelines

The hold time is essential in maintaining stable LDP sessions. If the router does not receive any LDP hello messages from the neighbor within the hold time, it will consider the session to be down and act accordingly.

Setting an appropriate hold time allows for timely detection of failures. If a neighbor becomes unreachable or there's a network issue, the configured hold time determines the timeout period after which the router will declare the neighbor unreachable.

Configure the hold time carefully. A very short hold time might lead to frequent session resets due to transient network issues. A very long hold time might delay the detection and recovery from genuine network issues.

Different networks and environments may have different requirements for session stability and failure recovery. Configuring the session hold time allows network administrators to tailor the behavior of LDP sessions to fit specific needs.

> **NOTE**:
>
> For the **session-holdtime** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Example

• Configure the hold time period for keepalive.

```
admin@XorPlus# set protocols mpls ldp neighbor 2.2.2.2 session-holdtime 210
admin@XorPlus# commit
```

set protocols mpls ldp neighbor ttl-security disable

The **set protocols mpls ldp neighbor ttl-security disable** command disables Generalized TTL Security Mechanism (GTSM), as specified in RFC 5082.

The **delete protocols mpls ldp neighbor ttl-security disable** command deletes the configuration.

Command Syntax

set protocols mpls ldp neighbor <*ip*> **ttl-security disable**

delete protocols mpls ldp neighbor <*ip*> **ttl-security**

Parameter

Parameter	Description
neighbor <*ip*>	Specifies the IPv4/IPv6 address of an LDP peer.

Usage Guidelines

Disabling TTL security means that the router will not enforce TTL checks for packets from this neighbor, potentially making the system less secure. TTL security is often used to mitigate spoofing attacks where an attacker attempts to establish an LDP session by sending fake packets with a manipulated TTL value.

This might be necessary if compatibility with older or certain specific devices that do not support TTL security is required.

NOTE:

The commands **set protocols mpls ldp neighbor** <*ip*> **ttl-security hops** <*integer*> and **set protocols mpls ldp neighbor** <*ip*> **ttl-security disable** cannot be configured simultaneously.

Example

- Disable Generalized TTL Security Mechanism (GTSM).

```
admin@PICOS# set protocols mpls ldp neighbor 2.2.2.2 ttl-security disable
admin@PICOS# commit
```

set protocols mpls ldp neighbor ttl-security hops

The **set protocols mpls ldp neighbor ttl-security hops** command enforces Generalized TTL Security Mechanism (GTSM), as specified in RFC 5082. With this command, only neighbors that are the specified number of hops away will be allowed to become neighbors. This command is mutually exclusive with ebgp-multihop.

By default, TTL hop is 0, indicating **ttl-security** is disabled.

The **delete protocols mpls ldp neighbor ttl-security hops** command deletes the configuration.

NOTE:

- The valid range of TTL values allowed for detection packets varies among devices from different vendors, including 1 to 255 and 1 to 64. Therefore, when interoperating with devices from other vendors, it is necessary to configure different hop values according to the implementation of the other vendor's devices. Otherwise, packets sent by the peer will be discarded, leading to interruption of the LDP session.
- The commands **set protocols mpls ldp neighbor** <*ip*> **ttl-security hops** <*integer*> and **set protocols mpls ldp neighbor** <*ip*> **ttl-security disable** cannot be configured simultaneously.

Command Syntax

set protocols mpls ldp neighbor <*ip*> **ttl-security hops** <*integer*>

delete protocols mpls ldp neighbor <*ip*> **ttl-security hops**

Parameter

Parameter	Description
neighbor <*ip*>	Specifies the IPv4/IPv6 address of an LDP peer.
hops <*integer*>	Specifies the maximum number of valid hops allowed by the GTSM function. That value is an integer which can be configured between 1 and 254. By default, TTL hop is 0, indicating **ttl-security** is disabled.

Example

- Configure GTSM valid hops.

```
admin@PICOS# set protocols mpls ldp neighbor 2.2.2.2 ttl-security hops 10
admin@PICOS# commit
```

set protocols mpls ldp interface

The **set protocols mpls ldp interface** command enables MPLS LDP on an L3 interface under IPv4/IPv6 address family. Required to be configured on all nodes in the MPLS area.

The **delete protocols mpls ldp interface** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} interface <*interface-name*>

delete protocols mpls ldp {ipv4-family|ipv6-family} interface <*interface-name*>

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.
interface <*interface-name*>	Specifies an L3 interface to enable MPLS LDP. The value could be a VLAN interface, loopback interface name, routed interface or sub-interface. By default, MPLS LDP is disabled on all the interfaces.

Example

- Enable MPLS LDP on interface vlan200 of IPv4 address family.

```
admin@PICOS# set protocols mpls ldp ipv4-family interface vlan200
admin@PICOS# commit
```

set protocols mpls ldp ttl-security disable (IP family)

The **set protocols mpls ldp ttl-security disable** command disables Generalized TTL Security Mechanism (GTSM) under IP address family, as specified in RFC 5082.

The **delete protocols mpls ldp ttl-security disable** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} ttl-security disable

delete protocols mpls ldp {ipv4-family|ipv6-family} ttl-security

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.

Example

- Disable Generalized TTL Security Mechanism (GTSM) under IP address family,

```
admin@PICOS# set protocols mpls ldp ipv4-family ttl-security disable
admin@PICOS# commit
```

set protocols mpls ldp label-local-advertise

The **set protocols mpls ldp label-local-advertise** command configures the label assigned for the penultimate router under the address family on the egress LSP. The **explicit-null** option assigns an explicit null label(0), to the penultimate router. If **explicit-null** option is not specified, or this command is not configured, the LSR assigns an implicit null label(3), to the penultimate router.

The **delete protocols mpls ldp label-local-advertise** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} label-local-advertise [explicit-null]

delete protocols mpls ldp {ipv4-family|ipv6-family} label-local-advertise

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.

Example

- Configure to assign an explicit null label for the penultimate router on the egress LSP.

```
admin@PICOS# set protocols mpls ldp ipv4-family label-local-advertise explicit-null
admin@PICOS# commit
```

set protocols mpls ldp label-local-allocate

The **set protocols mpls ldp label-local-allocate** command configures the triggering conditions for allocating labels under the address family. The **host-routes** option allocates labels for host routes only (/32 or /128). If **host-routes** option is not specified, or this command is not configured, the LSR allocates labels for all the routes.

The **delete protocols mpls ldp label-local-allocate** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} label-local-allocate [host-routes]

delete protocols mpls ldp {ipv4-family|ipv6-family} label-local-allocate

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.

Example

- The following command allocates labels for host routes only (/32).

```
admin@PICOS# set protocols mpls ldp ipv4-family label-local-allocate host-routes
admin@PICOS# commit
```

set protocols mpls ldp discovery transport-address

The **set protocols mpls ldp discovery transport-address** command configures MPLS LDP transmission address under the address family. This is a requisite configuration for MPLS LDP.

The **delete protocols mpls ldp discovery transport-address** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} discovery transport-address <*ip-address*>

delete protocols mpls ldp {ipv4-family|ipv6-family} discovery transport-address

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.
transport-address <*ip-address*>	Specifies the MPLS LDP transmission address. The value is an IPv4 or IPv6 address.

Usage Guidelines

This address is used as the source address in the Hello message of LDP link.
LDP session is based on TCP connection, when two LSRs want to establish an LDP session between them, they need to confirm the LDP transport address of the peer before they can establish a TCP connection.

Example

- Configure MPLS LDP transmission address under IPv4 address family.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery transport-address 2.2.2.2
admin@PICOS# commit
```

set protocols mpls ldp discovery hello-interval

The **set protocols mpls ldp discovery hello-interval** command configures the interval for sending Hello message.

The **delete protocols mpls ldp discovery hello-interval** command deletes the configuration.

Command Syntax

set protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery hello-interval** <*hello-interval*>

delete protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery hello-interval**

Parameter

Parameter	Description
ipv4-family|ipv6-family	Optional. Specifies the IP address family type.
hello-interval <*hello-interval*>	Specifies the interval for sending Hello message. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 5 seconds.

Usage Guidelines

LSR periodically sends Hello messages according to the interval for sending Hello message, notifying neighboring LSRs of its presence in the network and establishing a Hello adjacency relationship.
It is recommended to use the default value.

NOTEs：

- Before configuring the **discovery hello-interval** and **discovery hello-holdtime**, the **discovery transport-address** under the IP family must be configured first.
- The configuration of **discovery hello-interval** and **discovery hello-holdtime** based on the IP family takes precedence over the global configuration.
- For the **discovery hello-interval** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Example

- Configure the interval for sending Hello message.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery hello-interval 10
admin@PICOS# commit
```

set protocols mpls ldp discovery hello-holdtime

The **set protocols mpls ldp discovery hello-holdtime** command configures the Hello hold time.

The **delete protocols mpls ldp discovery hello-holdtime** command deletes the configuration.

Command Syntax

set protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery hello-holdtime** <*hello-holdtime*>

delete protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery hello-holdtime**

Parameter

Parameter	Description
ipv4-family|ipv6-family	Optional. Specifies the IP address family type.
hello-holdtime <*hello-holdtime*>	Specifies the Hello hold time. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 15 seconds.

Usage Guidelines

LDP peers that have established a Hello adjacency relationship periodically send Hello messages to signify their intention to maintain this adjacency. If no new Hello message is received before the Hello hold timer expires, the adjacency will be terminated.
It is recommended to use the default value.

NOTEs：

- Before configuring the **discovery hello-interval** and **discovery hello-holdtime**, the **discovery transport-address** under the IP family must be configured first.
- The configuration of **discovery hello-interval** and **discovery hello-holdtime** based on the IP family takes precedence over the global configuration.
- For the **discovery hello-holdtime** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Example

- Configure the Hello hold time.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery hello-holdtime 30
admin@PICOS# commit
```

set protocols mpls ldp discovery targeted-hello-interval

The **set protocols mpls ldp discovery targeted-hello-interval** command configures the time interval for sending Targeted hello messages.

The **delete protocols mpls ldp discovery targeted-hello-interval** command deletes the configuration.

Command Syntax

set protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery targeted-hello-interval** <*hello-interval*>

delete protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery targeted-hello-interval**

Parameter

Parameter	Description
ipv4-family|ipv6-family	Optional. Specifies the IP address family type.
targeted-hello-interval <*hello-interval*>	Specifies the time interval for sending Targeted hello messages. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 15 seconds.

Usage Guidelines

This command plays a crucial role in the LDP discovery process, which is essential for the establishment and maintenance of LDP sessions between routers.

A shorter Hello interval results in more frequent Hello messages. This can help in quicker detection of peers going down, which might be critical in high-availability environments. However, it increases the processing load on the router and the amount of control traffic.

NOTEs：

- Before configuring the **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime**, the **targeted-hello-accept** under the IP family must be enabled first.
- The configuration of **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime** based on the IP family takes precedence over the global configuration.
- For the **discovery targeted-hello-interval** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Example

- Configure the interval for sending Targeted hello messages.

```
admin@PICOS# set protocols mpls ldp discovery targeted-hello-interval 10
admin@PICOS# commit
```

set protocols mpls ldp discovery targeted-hello-holdtime

The **set protocols mpls ldp discovery targeted-hello-holdtime** command configures the Targeted hello hold time.

The **delete protocols mpls ldp discovery targeted-hello-holdtime** command deletes the configuration.

Command Syntax

set protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery targeted-hello-holdtime** <*holdtime*>

delete protocols mpls ldp [**ipv4-family|ipv6-family**] **discovery targeted-hello-holdtime**

Parameter

Parameter	Description
ipv4-family|ipv6-family	Optional. Specifies the IP address family type.
targeted-hello-holdtime <*holdtime*>	Specifies the Targeted hello hold time. The value is an integer which can be configured between 1 and 65535 seconds. The default value is 45 seconds. 65535 implies infinite.

Usage Guidelines

The hold time determines how long a router should consider a neighbor to be reachable after the last targeted Hello message is received.

The `targeted-hello-holdtime` parameter sets the amount of time (in seconds) that the router will wait after receiving the last Hello message before considering the neighbor as unreachable. If the router does not receive another Hello message from the neighbor within this period, it will consider the neighbor to be down and will tear down the LDP session associated with that neighbor.

This timer ensures that the LDP session is maintained as long as the neighbor is responsive. It is a fail-safe mechanism that helps in quickly detecting and reacting to network changes.

NOTEs：

- Before configuring the **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime**, the **targeted-hello-accept** under the IP family must be enabled first.
- The configuration of **discovery targeted-hello-interval** and **discovery targeted-hello-holdtime** based on the IP family takes precedence over the global configuration.
- For the **targeted-hello-holdtime** configuration, the actual effective timer value equals the smaller of the timers configured on both ends of the LDP peers.

Example

- Configure the Targeted hello hold time.

```
admin@PICOS# set protocols mpls ldp discovery targeted-hello-holdtime 50
admin@PICOS# commit
```

set protocols mpls ldp discovery targeted-hello-accept

The **set protocols mpls ldp discovery targeted-hello-accept** command is used to enable a router to accept targeted LDP Hello messages. These targeted Hello messages are sent from specific neighbors to establish targeted sessions.

> **NOTE**:
>
> Before configuring this command, the **discovery transport-address** must be configured first.

The **delete protocols mpls ldp discovery targeted-hello-accept** command deletes the configuration.

Command Syntax

set protocols mpls ldp {**ipv4-family|ipv6-family**} **discovery targeted-hello-accept** <**true** | **false**>

delete protocols mpls ldp {**ipv4-family|ipv6-family**} **discovery targeted-hello-accept**

Parameter

Parameter	Description
ipv4-family|ipv6-family	Required. Specifies the IP address family type.
<**true** | **false**>	Enables or disables the device to accept targeted LDP Hello messages. These targeted Hello messages are sent from specific neighbors to establish targeted sessions. The value could be **true** or **false**. • **true**: Enables the device to accept targeted LDP Hello messages. • **false**: Disable the device to accept targeted LDP Hello messages. The default value is **false**.

Example

- Enable the device to accept targeted LDP Hello messages.

```
admin@PICOS# set protocols mpls ldp ipv4-family discovery targeted-hello-accept true
admin@PICOS# commit
```

set protocols mpls ldp dual-stack transport-connection prefer-ipv4

The **set protocols mpls ldp dual-stack transport-connection prefer-ipv4** command configures to instruct the router to prefer IPv4 for the transport connection when establishing LDP sessions in a dual-stack environment where both IPv4 and IPv6 are enabled.

The **delete protocols mpls ldp dual-stack transport-connection** command deletes the configuration.

Command Syntax

set protocols mpls ldp dual-stack transport-connection prefer-ipv4

delete protocols mpls ldp dual-stack transport-connection

Parameter

Null.

Usage Guidelines

By default, routers running MPLS with LDP in a dual-stack environment use IPv6 for the transport connection. However, in certain scenarios, such as network interoperability requirements or specific operational preferences, it may be desirable to explicitly specify IPv4 as the preferred transport protocol.

Example

- Configure to instruct the router to prefer IPv4 for the transport connection when establishing LDP sessions in a dual-stack environment where both IPv4 and IPv6 are enabled.

```
admin@PICOS# set protocols mpls ldp dual-stack transport-connection prefer-ipv4
admin@PICOS# commit
```

set protocols mpls ldp dual-stack interop

The **set protocols mpls ldp dual-stack interop** command is used in a Cisco environment to enable the Label Distribution Protocol (LDP) to support dual-stack operation, allowing it to work with both IPv4 and IPv6 networks seamlessly. This command ensures interoperability between Cisco routers running LDP in environments where both IPv4 and IPv6 are used.

The **delete protocols mpls ldp dual-stack interop** command deletes the configuration.

Command Syntax

set protocols mpls ldp dual-stack interop

delete protocols mpls ldp dual-stack interop

Parameter

Null.

Example

- Enable the Label Distribution Protocol (LDP) to support dual-stack operation in a Cisco environment.

```
admin@PICOS# set protocols mpls ldp dual-stack interop
admin@PICOS# commit
```

set protocols mpls ldp targeted-neighbor

The **set protocols mpls ldp targeted-neighbor** command configures sending Targeted Hello messages to specified peers to establish LDP sessions proactively, allowing responses to Targeted Hello messages from specified peers.

The **delete protocols mpls ldp targeted-neighbor** command deletes the configuration.

Command Syntax

set protocols mpls ldp {ipv4-family|ipv6-family} targeted-neighbor *<ip-address>*

delete protocols mpls ldp {ipv4-family|ipv6-family} targeted-neighbor

Parameter

Parameter	Description
{ipv4-family|ipv6-family}	Required. Specifies the IP address family type.
targeted-neighbor *<ip-address>*	Specifies the Targeted peer IP. The value is an IPv4/IPv6 address.

Example

- Configure sending Targeted Hello messages to specified peers to establish LDP sessions proactively.

```
admin@PICOS# set protocols mpls ldp ipv4-family targeted-neighbor 2.2.2.2
admin@PICOS# commit
```

set protocols mpls ldp traceoption labels

The **set protocols mpls ldp traceoption labels** command can be used to enable MPLS LDP debugging for label configuration tracing.

The **delete protocols mpls ldp traceoption labels** command deletes the configuration.

Command Syntax

set protocols mpls ldp traceoption labels

delete protocols mpls ldp traceoption labels

Parameters

Null.

Example

- Enable MPLS LDP debugging for label configuration tracing.

```
admin@PICOS# set protocols mpls ldp traceoption labels
admin@PICOS# commit
```

set protocols mpls ldp traceoption errors

The **set protocols mpls ldp traceoption errors** command can be used to enable MPLS LDP debugging for errors tracing.

The **delete protocols mpls ldp traceoption errors** command deletes the configuration.

Command Syntax

set protocols mpls ldp traceoption errors

delete protocols mpls ldp traceoption errors

Parameters

Null.

Example

- Enable MPLS LDP debugging for errors tracing.

```
admin@PICOS# set protocols mpls ldp traceoption errors
admin@PICOS# commit
```

set protocols mpls ldp traceoption event

The **set protocols mpls ldp traceoption event** command can be used to enable MPLS LDP debugging for event tracing.

The **delete protocols mpls ldp traceoption event** command deletes the configuration.

Command Syntax

set protocols mpls ldp traceoption event

delete protocols mpls ldp traceoption event

Parameters

Null.

Example

- Enable MPLS LDP debugging for event tracing.

```
admin@PICOS# set protocols mpls ldp traceoption event
admin@PICOS# commit
```

set protocols mpls ldp traceoption discovery

The **set protocols mpls ldp traceoption discovery** command can be used to enable MPLS LDP debugging for discovery information tracing.

The **delete protocols mpls ldp traceoption discovery** command deletes the configuration.

Command Syntax

set protocols mpls ldp traceoption discovery

delete protocols mpls ldp traceoption discovery

Parameters

Null.

Example

- Enable MPLS LDP debugging for discovery information tracing.

```
admin@PICOS# set protocols mpls ldp traceoption discovery
admin@PICOS# commit
```

set protocols mpls ldp traceoption messages

The **set protocols mpls ldp traceoption messages** command can be used to enable MPLS LDP debugging for messages tracing.

The **delete protocols mpls ldp traceoption messages** command deletes the configuration.

Command Syntax

set protocols mpls ldp traceoption messages

delete protocols mpls ldp traceoption messages

Parameters

Null.

Example

- Enable MPLS LDP debugging for messages tracing.

```
admin@PICOS# set protocols mpls ldp traceoption messages
admin@PICOS# commit
```

run show mpls ldp binding

The **run show mpls ldp binding** command is used to view Label Information Base (LIB) information.

Command Syntax

run show mpls ldp [**ipv4**|**ipv6**] **binding**

Parameter

Parameter	Description
[**ipv4**|**ipv6**]	Optional. Specifies the IP address family type.

Example

- View Label Information Base (LIB) information.

```
admin@sw2# run show mpls ldp ipv6 binding
AF   Destination          Nexthop         Local Label Remote Label  In Use
ipv6 2::2/128             0.0.0.0         imp-null    -                no
ipv6 3::3/128             3.3.3.3         41          imp-null         yes
ipv6 3::3/128             5.5.5.5         41          21               no
ipv6 4::4/128             3.3.3.3         17          23               yes
ipv6 4::4/128             5.5.5.5         17          17               no
ipv6 5::5/128             3.3.3.3         18          17               no

admin@sw3# run show mpls ldp binding
AF   Destination          Nexthop         Local Label Remote Label  In Use
ipv4 10.36.15.0/24        0.0.0.0         imp-null    -                no
ipv6 2::2/128             2.2.2.2         16          imp-null         yes
ipv6 2::2/128             5.5.5.5         16          16               no
ipv6 3::3/128             0.0.0.0         imp-null    -                no
ipv6 4::4/128             4.4.4.4         23          imp-null         yes
ipv6 5::5/128             2.2.2.2         17          18               no
```

In the show result, the parameter "`In Use`" indicates whether the label binding entry is effective or not.

- **yes**: indicates the label binding entry is effective.
- **no**: indicates the label binding entry is ineffective.

run show mpls ldp neighbor

The **run show mpls ldp neighbor** command is used to view the information of the MPLS neighbors discovered. The **detail** option shows comprehensive information about an LDP session, including session authentication, state, message statistics and LDP discovery source information. The **capabilities** option shows the neighbor capabilities information.

Command Syntax

run show mpls ldp neighbor [<*neighbor-router-id*>] [**detail**] [**capabilities**]

Parameter

Parameter	Description
<*neighbor-router-id*>	Optional. Specifies the neighbor LDP router ID in A.B.C.D format.

Example

- View the information of the MPLS neighbors discovered.

```
admin@sw3# run show mpls ldp neighbor
AF   ID              State       Remote Address    Uptime
ipv6 2.2.2.2         OPERATIONAL 2::2            3d01h33m
ipv6 4.4.4.4         OPERATIONAL 4::4            3d01h32m
ipv6 5.5.5.5         OPERATIONAL 5::5            3d01h32m


admin@sw3# run show mpls ldp neighbor 2.2.2.2
AF   ID              State       Remote Address    Uptime
ipv6 2.2.2.2         OPERATIONAL 2::2            3d01h33m
```

The state of an LDP session are as follows:

- **PRESENT**: This represents the initial state of the LDP session. In this state, both parties exchange Hello messages, and upon receiving the TCP connection establishment event, the session transitions to the **INITIALIZED** state.
- **INITIALIZED**: This indicates that the LDP session is in the initialization phase.
- **OPENSENT**: After entering the **INITIALIZED** state, the active party sends an *Initialized* message to the passive party and waits for a response.
- **OPENREC**: After entering the **INITIALIZED** state, when both parties have received the *Keepalive* message from each other, the LDP session transitions to the **OPERATIONAL** state.
- **OPERATIONAL**: This indicates that the LDP session has been successfully established.

- View the information of the MPLS neighbors discovered in detail.

```
admin@sw3# run show mpls ldp neighbor 2.2.2.2 detail
Peer LDP Identifier: 2.2.2.2:0
  TCP connection: 3::3:34795 - 2::2:646
  Authentication: none
  Session Holdtime: 180 secs; KeepAlive interval: 60 secs
  State: OPERATIONAL; Downstream-Unsolicited
```

```
  Up time: 3d01h33m
  Messages sent/rcvd:
   - Keepalive Messages: 4409/4404
   - Address Messages: 3/7
   - Address Withdraw Messages: 3/8
   - Notification Messages: 0/0
   - Capability Messages: 0/0
   - Label Mapping Messages: 89/158
   - Label Request Messages: 0/0
   - Label Withdraw Messages: 13/21
   - Label Release Messages: 21/13
   - Label Abort Request Messages: 0/0
  Capabilities Sent:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  Capabilities Received:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  LDP Discovery Sources:
    IPv6:
      Interface: vlan30


admin@sw3# run show mpls ldp neighbor detail
Peer LDP Identifier: 2.2.2.2:0
  TCP connection: 3::3:34795 - 2::2:646
  Authentication: none
  Session Holdtime: 180 secs; KeepAlive interval: 60 secs
  State: OPERATIONAL; Downstream-Unsolicited
  Up time: 3d01h33m
  Messages sent/rcvd:
   - Keepalive Messages: 4409/4404
   - Address Messages: 3/7
   - Address Withdraw Messages: 3/8
   - Notification Messages: 0/0
   - Capability Messages: 0/0
   - Label Mapping Messages: 89/158
   - Label Request Messages: 0/0
   - Label Withdraw Messages: 13/21
   - Label Release Messages: 21/13
   - Label Abort Request Messages: 0/0
  Capabilities Sent:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  Capabilities Received:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  LDP Discovery Sources:
    IPv6:
      Interface: vlan30

Peer LDP Identifier: 4.4.4.4:0
  TCP connection: 3::3:646 - 4::4:33289
  Authentication: none
```

```
  Session Holdtime: 180 secs; KeepAlive interval: 60 secs
  State: OPERATIONAL; Downstream-Unsolicited
  Up time: 3d01h33m
  Messages sent/rcvd:
   - Keepalive Messages: 4409/4410
   - Address Messages: 3/1
   - Address Withdraw Messages: 3/3
   - Notification Messages: 0/0
   - Capability Messages: 0/0
   - Label Mapping Messages: 106/4
   - Label Request Messages: 0/0
   - Label Withdraw Messages: 10/10
   - Label Release Messages: 10/10
   - Label Abort Request Messages: 0/0
  Capabilities Sent:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  Capabilities Received:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  LDP Discovery Sources:
    IPv6:
      Interface: vlan10

Peer LDP Identifier: 5.5.5.5:0
  TCP connection: 3::3:646 - 5::5:39257
  Authentication: none
  Session Holdtime: 180 secs; KeepAlive interval: 60 secs
  State: OPERATIONAL; Downstream-Unsolicited
  Up time: 3d01h33m
  Messages sent/rcvd:
   - Keepalive Messages: 4409/4408
   - Address Messages: 3/4
   - Address Withdraw Messages: 3/5
   - Notification Messages: 0/0
   - Capability Messages: 0/0
   - Label Mapping Messages: 43/90
   - Label Request Messages: 0/0
   - Label Withdraw Messages: 10/21
   - Label Release Messages: 21/10
   - Label Abort Request Messages: 0/0
  Capabilities Sent:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  Capabilities Received:
   - Dynamic Announcement (0x0506)
   - Typed Wildcard (0x050B)
   - Unrecognized Notification (0x0603)
  LDP Discovery Sources:
    IPv6:
      Interface: vlan20


admin@sw3# run show mpls ldp neighbor capabilities
Peer LDP Identifier: 2.2.2.2:0
```

```
  Capabilities Sent:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)
  Capabilities Received:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)

Peer LDP Identifier: 4.4.4.4:0
  Capabilities Sent:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)
  Capabilities Received:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)

Peer LDP Identifier: 5.5.5.5:0
  Capabilities Sent:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)
  Capabilities Received:
    - Dynamic Announcement (0x0506)
    - Typed Wildcard (0x050B)
    - Unrecognized Notification (0x0603)
```

run show mpls ldp interface

The **run show mpls ldp interface** command is used to view interface information that enables LDP.

Command Syntax

run show mpls ldp [ipv4|ipv6] interface

Parameter

Parameter	Description
[**ipv4**|**ipv6**]	Optional. Specifies the IP address family type.

Example

- View interface information that enables LDP.

```
admin@sw3# run show mpls ldp interface
AF   Interface   State  Uptime   Hello Timers  ac
ipv6 vlan10      ACTIVE 2d23h56m 5/15           1
ipv6 vlan20      ACTIVE 2d23h56m 5/15           1
ipv6 vlan30      ACTIVE 2d23h56m 5/15           1
ipv6 vlan40      DOWN   00:00:00 5/15           0


admin@sw3# run show mpls ldp ipv6 interface
AF   Interface   State  Uptime   Hello Timers  ac
ipv6 vlan10      ACTIVE 2d23h56m 5/15           1
ipv6 vlan20      ACTIVE 2d23h56m 5/15           1
ipv6 vlan30      ACTIVE 2d23h56m 5/15           1
ipv6 vlan40      DOWN   00:00:00 5/15           0
```

run show mpls forward-table

The **run show mpls forward-table** command shows the MPLS label forward table information.

Command Syntax

run show mpls forward-table {all | nexthop <*nexthop***> | outlabel <***outlabel***>}**

Parameter

Parameter	Description
all	Shows all of the MPLS label forward table.
nexthop <*nexthop***>**	Shows MPLS label forward table of specified next-hop address information.
outlabel <*outlabel***>**	Shows MPLS label forward table of specified out label information.

Example

- View the MPLS label forward table information.

```
admin@sw2# run show mpls forward-table all
In-label  Out-label  Outgoing-Interface  Next-Hop                       Route-Ref  If-Id  Egress-Id  Inuse
--------  ---------  ------------------  -----------------------------  ---------  -----  ---------  -----
NULL      23         vlan30              fe80::669d:9920:8d2:5aff       1          8197   100009     yes
20        imp-null   vlan30              fe80::669d:9920:8d2:5aff       0          8203   100016     yes
41        imp-null   vlan30              fe80::669d:9920:8d2:5aff       0          8203   100016     yes
17        23         vlan30              fe80::669d:9920:8d2:5aff       0          8201   100022     yes
18        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes
21        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes


admin@sw2# run show mpls forward-table nexthop fe80::c2b8:e620:374:34e9
In-label  Out-label  Outgoing-Interface  Next-Hop                       Route-Ref  If-Id  Egress-Id  Inuse
--------  ---------  ------------------  -----------------------------  ---------  -----  ---------  -----
18        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes
21        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes


admin@sw2# run show mpls forward-table outlabel 3
In-label  Out-label  Outgoing-Interface  Next-Hop                       Route-Ref  If-Id  Egress-Id  Inuse
--------  ---------  ------------------  -----------------------------  ---------  -----  ---------  -----
20        imp-null   vlan30              fe80::669d:9920:8d2:5aff       0          8203   100016     yes
41        imp-null   vlan30              fe80::669d:9920:8d2:5aff       0          8203   100016     yes
18        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes
21        imp-null   vlan20              fe80::c2b8:e620:374:34e9       0          8202   100018     yes


admin@sw2# run show mpls forward-table outlabel 3 nexthop fe80::c2b8:e620:374:34e9
In-label  Out-label  Outgoing-Interface  Next-Hop                       Route-Ref  If-Id  Egress-Id  Inuse
```

```
--------  ---------  ------------------  ------------------------------  ---------  -----  ---------  -----
18        imp-null   vlan20              fe80::c2b8:e620:374:34e9        0          8202   100018     yes
21        imp-null   vlan20              fe80::c2b8:e620:374:34e9        0          8202   100018     yes
```

run show mpls egress interface

The **run show mpls egress interface** command shows a list of egress interfaces and the associated parameters information.

Command Syntax

run show mpls egress interface

Parameter

None.

Example

- View the Label Switched Path (LSP) table on a MPLS device.

```
admin@sw2# run show mpls egress interface
MAC address         If-name   Egress-id   Ref-count   Out-label   Label-action   Next-hop
-----------------   -------   ---------   ---------   ---------   ------------   --------
64:9d:99:d2:5a:ff   xe-1/1/2  100012      41          imp-null    SWAP           fe80::669d:9920:3d2:5aff
64:9d:99:d2:5a:ff   xe-1/1/2  100008      3           -           NULL           -
64:9d:99:d2:5a:ff   xe-1/1/2  100016      5           imp-null    SWAP           fe80::669d:9920:8d2:5aff
64:9d:99:d2:5a:ff   xe-1/1/2  100022      1           23          SWAP           fe80::669d:9920:8d2:5aff
64:9d:99:d2:5a:ff   xe-1/1/2  100009      2           23          PUSH           fe80::669d:9920:8d2:5aff
c0:b8:e6:74:34:e9   xe-1/1/3  100013      25          imp-null    SWAP           fe80::c2b8:e620:174:34e9
c0:b8:e6:74:34:e9   xe-1/1/3  100015      6           imp-null    SWAP           fe80::c2b8:e620:174:34e9
c0:b8:e6:74:34:e9   xe-1/1/3  100020      0           20          SWAP           fe80::c2b8:e620:174:34e9
c0:b8:e6:74:34:e9   xe-1/1/3  100007      3           -           NULL           -
c0:b8:e6:74:34:e9   xe-1/1/1  100010      3           -           NULL           -
c0:b8:e6:74:34:e9   xe-1/1/1  100018      2           imp-null    SWAP           fe80::c2b8:e620:374:34e9
```

run show mpls table

The **run show mpls table** command shows the Label Switched Path (LSP) table on a MPLS device.

Command Syntax

run show mpls table [*<in-label>*]

Parameter

Parameter	Description
[*<in-label>*]	Optional. Specifies the MPLS label used when a packet enters the device.The value is an integer.

Example

- View the Label Switched Path (LSP) table on a MPLS device.

```
admin@sw2# run show mpls table
Inbound Label  Type  Nexthop                   Outbound Label
 ---------------------------------------------------------------
 17             LDP   fe80::669d:9920:8d2:5aff  23
 18             LDP   fe80::c2b8:e620:374:34e9  implicit-null
 18             LDP   fe80::c2b8:e620:174:34e9  implicit-null
 20             LDP   fe80::669d:9920:8d2:5aff  implicit-null
 21             LDP   fe80::c2b8:e620:374:34e9  implicit-null
 21             LDP   fe80::c2b8:e620:174:34e9  implicit-null
 21             LDP   fe80::669d:9920:8d2:5aff  implicit-null
 41             LDP   fe80::669d:9920:8d2:5aff  implicit-null


admin@sw2# run show mpls table 21
Local label: 21 (installed)
 type: LDP remote label: 3 distance: 150
  via fe80::c2b8:e620:374:34e9 dev vlan20 (installed)
 type: LDP remote label: 3 distance: 150
  via fe80::c2b8:e620:174:34e9 dev vlan10 (installed)
 type: LDP remote label: 3 distance: 150
  via fe80::669d:9920:8d2:5aff dev vlan30 (installed)
```

run show mpls interface

The **run show mpls interface** command is used to view the label information per interface that enables MPLS.

Command Syntax

run show mpls interface [**outlabel** <*outlabel*>]

Parameter

Parameter	Description
outlabel <*outlabel*>	Optional. Specifies the MPLS out label.

Example

- View the label information per interface that enables MPLS.

```
admin@sw2# run show mpls interface
Interface     If-id    Out-label   Ref-count
---------     ------   ---------   ---------
vlan10        8205     3           6
vlan20        8202     3           2
vlan30        8203     3           2
vlan30        8197     23          1
vlan30        8201     23          1


admin@sw2# run show mpls interface outlabel 23
Interface     If-id    Out-label   Ref-count
---------     ------   ---------   ---------
vlan30        8197     23          1
vlan30        8201     23          1
```

run show mpls status

The **run show mpls status** command shows whether MPLS is enabled on the device.

Command Syntax

run show mpls status

Parameter

None.

Example

- View whether MPLS is enabled on the device.

```
admin@sw3# run show mpls status
MPLS support enabled: yes
```

run show mpls label

The **run show mpls label** command shows the list of routes that reference MPLS label.

Command Syntax

run show mpls label <*label*>

Parameter

Parameter	Description
label <*label*>	Specifies the MPLS label.The value is an integer.

Example

- View the Label Switched Path (LSP) table on a MPLS device.

```
admin@sw2# run show mpls label 23
Route-List:
4::4/128
```

run show mpls ldp discovery

The **run show mpls ldp discovery** command is used to view Discovery Hello Information. The **detail** option can be used to show details of Discovery Hello Information.

Command Syntax

run show mpls ldp [ipv4|ipv6] discovery [**detail**]

Parameter

Parameter	Description
[**ipv4**|**ipv6**]	Optional. Specifies the IP address family type.

Example

- View Discovery Hello Information.

```
admin@sw3# run show mpls ldp discovery
AF   ID              Type     Source           Holdtime
ipv6 2.2.2.2         Link     vlan30                 15
ipv6 4.4.4.4         Link     vlan10                 15
ipv6 5.5.5.5         Link     vlan20                 15


admin@sw3# run show mpls ldp discovery detail
Local:
  LSR Id: 3.3.3.3:0
  Transport Address (IPv6): 3::3
Discovery Sources:
  Interfaces:
    vlan10:
      LSR Id: 4.4.4.4:0
          Source address: fe80::6a21:5f20:1a7:7163
          Transport address: 4::4
          Hello hold time: 15 secs (due in 13 secs)
          Dual-stack capability TLV: no
    vlan20:
      LSR Id: 5.5.5.5:0
          Source address: fe80::c2b8:e620:274:34e9
          Transport address: 5::5
          Hello hold time: 15 secs (due in 13 secs)
          Dual-stack capability TLV: no
    vlan30:
      LSR Id: 2.2.2.2:0
          Source address: fe80::1eea:b20:cff:fcb9
          Transport address: 2::2
          Hello hold time: 15 secs (due in 13 secs)
          Dual-stack capability TLV: no
  Targeted Hellos:
```

run show mpls fec

The **run show mpls fec** command shows the MPLS FEC table.

Command Syntax

run show mpls fec [<*ip-address/prefixlen*>]

Parameter

Parameter	Description
[<*ip-address/prefixlen*>]	Optional. Specifies the MPLS FEC.The value is an IPv4/IPv6 network with mask. For example: 1.1.1.0/24

Example

- View the MPLS FEC table.

```
admin@PICOS# run show mpls fec 10.10.10.0/24
10.10.10.0/24
  Label: 500
```

Loopback Detection Commands

- set protocols loopback-detection enable
- set protocols loopback-detection interface enable
- set protocols loopback-detection message-interval
- set protocols loopback-detection traceoptions configuration disable
- set protocols loopback-detection traceoptions all disable
- run show loopback-detection
- run clear loopback-detection interface

set protocols loopback-detection enable

The **set protocols loopback-detection enable** command can be used to enable or disable loopback detection function globally.

The **delete protocols loopback-detection enable** command deletes the configuration.

> **NOTE:**
>
> To enable the loopback detection function, users need to enable loopback detection BOTH globally and at the per-interface level. The command **set protocols loopback-detection interface** <*interface-name*> **enable** <**true | false**> can be used to enable loopback detection function on a specific interface.

Command Syntax

set protocols loopback-detection enable <**true | false**>

delete protocols loopback-detection enable

Parameter

Parameter	Description
enable <**true	false**>	Enable or disable loopback detection function globally. The value could be **true** or **false**. • **true**: Enable loopback detection function globally. • **false**: Disable loopback detection function globally. By default, loopback detection function is disabled.

Example

- Enable loopback detection function globally.

```
admin@PICOS# set protocols loopback-detection enable true
admin@PICOS# commit
```

set protocols loopback-detection interface enable

The **set protocols loopback-detection interface enable** command can be used to enable or disable loopback detection function on a specific interface.

The **delete protocols loopback-detection interface enable** command deletes the configuration.

NOTE:

To enable the loopback detection function, users need to enable loopback detection BOTH globally and at the per-interface level. The command **set protocols loopback-detection enable** <**true | false**> can be used to enable loopback detection function globally.

Command Syntax

set protocols loopback-detection interface <*interface-name*> **enable** <**true | false**>

delete protocols loopback-detection interface <*interface-name*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value is a physical interface or an LAG interface.
enable <**true	false**>	Enable or disable loopback detection function on a specific interface. The value could be **true** or **false**. • **true**: Enable loopback detection function on a specific interface. • **false**: Disable loopback detection function on a specific interface. By default, interface-based loopback detection function is disabled. **NOTE**: Loopback detection can be enabled on a physical interface or a LAG interface but cannot be enabled on the member interface of a LAG interface.

Example

- Enable loopback detection function on interface te-1/1/7.

```
admin@PICOS# set protocols loopback-detection enable true
admin@PICOS# set protocols loopback-detection interface te-1/1/7 enable true
admin@PICOS# commit
```

set protocols loopback-detection message-interval

The **set protocols loopback-detection message-interval** command configures the interval between sending loopback detection messages.

The **delete protocols loopback-detection message-interval** command deletes the configuration.

Command Syntax

set protocols loopback-detection message-interval <*message-interval*>

delete protocols loopback-detection message-interval

Parameter

Parameter	Description
message-interval <*message-interval*>	Specifies the interval between sending loopback detection messages. The value is an integer, in second, that ranges from 10 to 60. The default value is 30 seconds.

Example

- Configure the interval between sending loopback detection messages to 15 seconds.

```
admin@PICOS# set protocols loopback-detection message-interval 15
admin@PICOS# commit
```

set protocols loopback-detection traceoptions configuration disable

The **set protocols loopback-detection traceoptions configuration disable** command can be used to enable or disable loopback detection debugging for configuration tracing.

The **delete protocols loopback-detection traceoptions configuration disable** command deletes the configuration.

Command Syntax

set protocols loopback-detection traceoptions configuration disable <**true | false**>

delete protocols loopback-detection traceoptions configuration disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable loopback detection debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable loopback detection debugging for configuration tracing. • **false**: Enable loopback detection debugging for configuration tracing. By default, loopback detection debugging for configuration tracing is disabled.

Example

- Enable loopback detection debugging for configuration tracing.

```
admin@PICOS# set protocols loopback-detection traceoptions config disable false
admin@PICOS# commit
```

set protocols loopback-detection traceoptions all disable

The **set protocols loopback-detection traceoptions all disable** command can be used to enable or disable loopback detection debugging for tracing all the loopback-detection operations.

The **delete protocols loopback-detection traceoptions all disable** command deletes the configuration.

Command Syntax

set protocols loopback-detection traceoptions all disable <**true | false**>

delete protocols loopback-detection traceoptions all disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable loopback detection debugging for tracing all the loopback-detection operations. The value could be **true** or **false**. • **true**: Disable loopback detection debugging for tracing all the loopback-detection operations. • **false**: Enable loopback detection debugging for tracing all the loopback-detection operations. By default, loopback detection debugging for tracing all the loopback-detection operations is disabled.

Example

- Enable loopback detection debugging for tracing all the loopback-detection operations.

```
admin@PICOS# set protocols loopback-detection traceoptions all disable false
admin@PICOS# commit
```

run show loopback-detection

The **run show loopback-detection** command is used to view the configuration information and status information of loopback detection.

Command Syntax

run show loopback-detection

Parameter

None.

Example

- View the configuration information and status information of loopback detection.

```
admin@PICOS# run show loopback-detection
Loopback-detection: enabled
message-interval: 30s

Interface       LBD Tx    Status                From_Port
----------      ----------    ------------          -----------
ge-1/1/1        true          Normal
ge-1/1/2        false         LoopDetected    ge-1/1/1
......
```

Field	Description
Loopback-detection	Indicates whether loopback detection is globally enabled.
message-interval	Indicates the interval between sending loopback detection packets, in seconds.
Interface	All the physical interfaces or LAG interfaces on the device are displayed.
LBD Tx	Indicate whether the interface is the sending interface of the Loopback Detection (LBD) message, the value could be **true** or **false**. • **true**: indicates that the interface is the sending interface of the Loopback Detection (LBD) message. • **false**: indicates that the interface is not the sending interface of the Loopback Detection (LBD) message.
Status	If an interface receives a Loopback Detection (LBD) message sent from this device, then a loopback is detected, the Status of this interface is **LoopDetected**. The Status of other interfaces are **Normal**.
From_Port	When a loopback is detected, this field indicates the sending interface of loopback detection packets.

run clear loopback-detection interface

The **run clear loopback-detection interface** command is used to clear the ***err-disable*** state of the loopback detection interface.

Command Syntax

run clear loopback-detection interface {<*interface-name*> | **all**}

Parameter

Parameter	Description
interface {<*interface-name*> | **all**}	Specifies the interface name. The value is a physical interface or an LAG interface. If **all** is specified, clear the ***err-disable*** state for all the loopback detection interfaces.

Example

- Clear the ***err-disable*** state of the loopback detection interface xe-1/1/1.

```
admin@PICOS# run clear loopback-detection interface xe-1/1/1
Clear xe-1/1/1 err-disable state
```